REPEAT PROCESSOR AND ITS METHOD

Patent number: JP2003229900
Publication date: 2003-08-15
Inventor: NAGASHIMA MASARU
Applicant: MITSUBISHI ELECTRIC CORP
Classification:
- international: ***H04L12/46; H04L12/56;*** **H04L12/46; H04L12/56;** (IPC1-7): H04L12/56; H04L12/46
- european:
Application number: JP20020026581 20020204
Priority number(s): JP20020026581 20020204

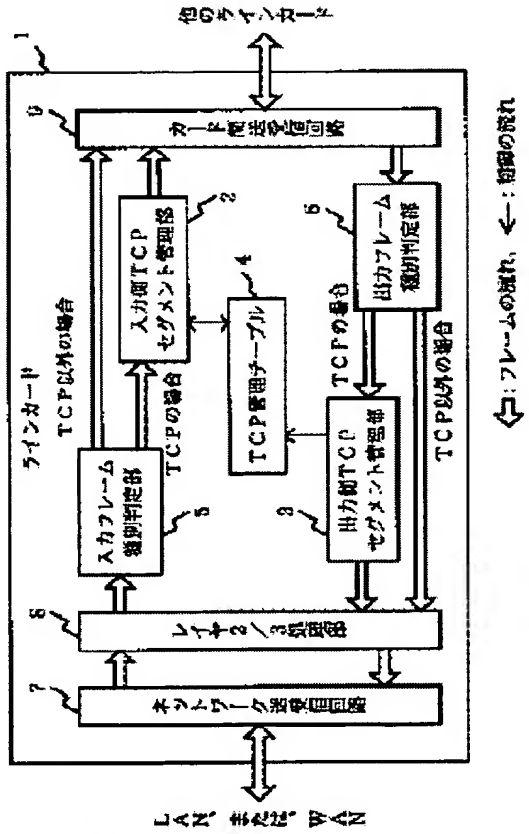
Report a data error here

Abstract of **JP2003229900**

PROBLEM TO BE SOLVED: To improve the utilization efficiency of a network by canceling invalid packets such as a packet of data omission.

SOLUTION: In a plurality of line cards 1 loaded in an IP router, a TCP management table 4 stores the sequence number of a packet to be received next as a Seq number and stores the sequence number of a latest packet received by the packet receiving side as an Ack number and an input side TCP segment management part 2 receives a packet transmitted by a LAN or the like through a network transmitting/receiving circuit 7 or the like, compares the sequence number of the received IP packet with the Seq number and the Ack number stored in the table 4, and when the value of the sequence number is not less than the Ack number and not more than the Seq number, updates the Seq number stored in the table 4 to the sequence number of the packet to be received next, transmits the sequence number to another line card 1 through an inter-card transmitting/receiving circuit 9, and cancels the received packet.

COPYRIGHT: (C)2003,JPO



Data supplied from the ***esp@cenet*** database - Worldwide

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号
特開2003－229900
（P2003－229900A）
(43)公開日　平成15年８月15日(2003.8.15)

(51)Int.Cl.⁷	識別記号	ＦＩ		テーマコード（参考）
Ｈ０４Ｌ　12/56	２００	Ｈ０４Ｌ　12/56	２００Ｚ	５Ｋ０３０
12/46		12/46	Ｅ	５Ｋ０３３
	１００		１００Ｒ	
	２００		２００Ｓ	

審査請求　未請求　請求項の数16　ＯＬ　（全 26 頁）

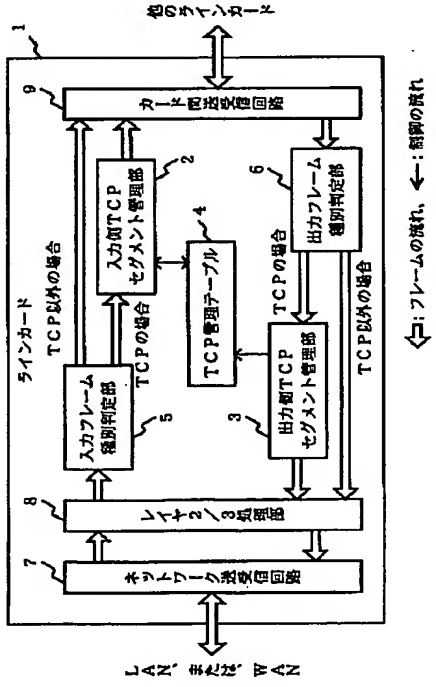
(21)出願番号　特願2002－26581(P2002－26581)
(22)出願日　平成14年２月４日(2002.2.4)

(71)出願人　000006013
三菱電機株式会社
東京都千代田区丸の内二丁目２番３号
(72)発明者　長島　勝
東京都千代田区丸の内二丁目２番３号　三菱電機株式会社内
(74)代理人　100099461
弁理士　溝井　章司　（外５名）

Ｆターム(参考)　5K030 HA08 HC01 HC14 HD03 HD05 HD06 JA05 KA04 LA02 MB13 MB18
5K033 CB08 CC01 DA06 DB12 DB18

(54)【発明の名称】　中継処理装置及び中継処理方法

(57)【要約】
【課題】　データ抜け等の無効なパケットを廃棄し、ネットワークの利用効率を向上させる。
【解決手段】　ＩＰルータ内に複数枚実装されたラインカード１において、ＴＣＰ管理テーブル４には次に受信するパケットのシーケンス番号がＳｅｑ番号として記憶され、パケットの受信側が受信した最新のパケットのシーケンス番号がＡｃｋ番号として記憶されており、入力側ＴＣＰセグメント管理部２は、ＬＡＮ等より送信されたパケットをネットワーク送受信回路７等を介して受信し、受信したＩＰパケットのシーケンス番号とＴＣＰ管理テーブル４内のＳｅｑ番号、Ａｃｋ番号とを比較し、シーケンス番号の値がＡｃｋ番号以上の値であってＳｅｑ番号以下の値である場合には、ＴＣＰ管理テーブル４内のＳｅｑ番号を次に受信するパケットのシーケンス番号に更新してカード間送受信回路９を介して他のラインカードに送信し、その他の場合には受信したパケットを廃棄する。



1

【特許請求の範囲】

【請求項１】　それぞれに少なくとも一つ以上の通信装置を有する複数のネットワークに接続された中継装置内で、前記複数のネットワークのうち特定のネットワークに関する中継処理を行う中継処理装置であって、

前記特定のネットワーク内の通信装置である特定ネットワーク通信装置から他のネットワーク内の通信装置である他ネットワーク通信装置に対して送信されたデータパケットであって、送信シーケンス番号として所定のシーケンス番号が付与されたデータパケットを順次受信する第一の通信処理部と、

データパケットに対する中継処理の要否判断の基準となるシーケンス番号を判断基準シーケンス番号として記憶する通信管理テーブルと、

前記第一の通信処理部によりデータパケットが受信される度に、受信された受信データパケットの送信シーケンス番号と前記通信管理テーブルに記憶された判断基準シーケンス番号とを比較して前記受信データパケットについて中継処理の要否判断を行う中継要否判断部と、

前記中継要否判断部により中継処理の対象とされた受信データパケットを前記他ネットワーク通信装置に対して送信する第二の通信処理部とを有することを特徴とする中継処理装置。

【請求項２】　前記中継要否判断部は、受信データパケットを中継処理の対象とする度に、中継処理の対象とした受信データパケットの次に中継処理の対象となるデータパケットの送信シーケンス番号を次中継シーケンス番号として算出し、次中継シーケンス番号を算出する度に新たに算出した次中継シーケンス番号に更新しながら前記通信管理テーブルに次中継シーケンス番号を登録し、

前記第二の通信処理部は、前記他ネットワーク通信装置がデータパケットを受信した場合に送達確認のために前記他ネットワーク通信装置から前記特定ネットワーク通信装置に対して送信された送達確認パケットであって、確認シーケンス番号として所定のシーケンス番号が付与された送達確認パケットを順次受信し、

前記中継処理装置は、更に、前記第二の通信処理部により送達確認パケットが受信される度に新たに受信された送達確認パケットの確認シーケンス番号に更新しながら前記通信管理テーブルに確認シーケンス番号を登録する送達確認パケット管理部を有し、

前記通信管理テーブルは、前記判断基準シーケンス番号として、前記中継要否判断部により最新に登録された次中継シーケンス番号と前記送達確認パケット管理部により最新に登録された確認シーケンス番号とを記憶し、

前記中継要否判断部は、前記第一の通信処理部によりデータパケットが受信される度に、受信データパケットの送信シーケンス番号を、前記通信管理テーブルに記憶されている次中継シーケンス番号及び確認シーケンス番号のうち少なくともいずれか一つと比較して前記受信データパケットについて中継処理の要否判断を行うことを特徴とする請求項１に記載の中継処理装置。

2

【請求項３】　前記中継要否判断部は、前記第一の通信処理部によりデータパケットが受信される度に、受信データパケットの送信シーケンス番号と前記通信管理テーブルに記憶されている確認シーケンス番号とを比較し、前記受信データパケットの送信シーケンス番号の値が前記通信管理テーブルに記憶されている確認シーケンス番号の値以上である場合に、前記受信データパケットの送信シーケンス番号と前記通信管理テーブルに記憶されている次中継シーケンス番号とを比較し、前記受信データパケットの送信シーケンス番号の値が前記通信管理テーブルに記憶されている次中継シーケンス番号の値以下である場合に、前記受信データパケットを中継処理の対象とすることを特徴とする請求項２に記載の中継処理装置。

【請求項４】　前記中継要否判断部は、前記受信データパケットの送信シーケンス番号の値が前記通信管理テーブルに記憶されている確認シーケンス番号の値未満であった場合及び前記受信データパケットの送信シーケンス番号の値が前記通信管理テーブルに記憶されている次中継シーケンス番号の値よりも大きい場合に、前記受信データパケットの廃棄を決定することを特徴とする請求項３に記載の中継処理装置。

【請求項５】　前記中継要否判断部は、中継処理の対象となった中継対象データパケットの送信シーケンス番号に前記中継対象データパケットのデータサイズを加算した値を前記次中継シーケンス番号として算出し、

前記第二の通信処理部は、前記他ネットワーク通信装置が受信した受信済データパケットの送信シーケンス番号に前記受信済データパケットのデータサイズを加算した値を前記確認シーケンス番号とする送達確認パケットを受信することを特徴とする請求項２に記載の中継処理装置。

【請求項６】　前記通信管理テーブルは、前記特定ネットワーク通信装置の識別子及び前記他ネットワーク通信装置の識別子をコネクション識別子情報として記憶しており、前記中継要否判断部により最新に登録された次中継シーケンス番号と前記送達確認パケット管理部により最新に登録された確認シーケンス番号とを前記コネクション識別子情報に対応づけて記憶し、

前記第一の通信処理部は、前記特定ネットワーク通信装置の識別子及び前記他ネットワーク通信装置の識別子を含むデータパケットを順次受信し、

前記中継要否判断部は、前記第一の通信処理部によりデータパケットが受信される度に、受信データパケットに含まれた前記特定ネットワーク通信装置の識別子及び前記他ネットワーク通信装置の識別子に対応するコネクション識別子情報を前記通信管理テーブル内で検索し、検索したコネクション識別子情報に対応づけられた次中継

シーケンス番号及び確認シーケンス番号のうち少なくともいずれか一つと前記受信データパケットの送信シーケンス番号とを比較して前記受信データパケットについて中継処理の要否判断を行うことを特徴とする請求項２に記載の中継処理装置。

【請求項７】　前記第一の通信処理部は、前記データパケットの受信に先立ち、前記特定ネットワーク通信装置の識別子及び前記他ネットワーク通信装置の識別子を含み、前記特定ネットワーク通信装置と前記他ネットワーク通信装置との間の通信コネクションの設定のために前記特定ネットワーク通信装置より送信されたコネクション設定パケットを受信し、

前記通信管理テーブルは、前記第一の通信処理部により前記コネクション設定パケットが受信された場合に、受信された前記コネクション設定パケットに含まれた前記特定ネットワーク通信装置の識別子及び前記他ネットワーク通信装置の識別子をコネクション識別子情報として記憶し、

前記第二の通信処理部は、前記コネクション設定パケットを前記他ネットワーク通信装置へ送信するとともに、前記特定ネットワーク通信装置の識別子及び前記他ネットワーク通信装置の識別子を含み、前記コネクション設定パケットに対する応答として前記他ネットワーク通信装置より送信された応答コネクション設定パケットを受信し、

前記中継処理装置は、更に、前記第二の通信処理部により前記応答コネクション設定パケットが受信された場合に、前記応答コネクション設定パケットに含まれた前記特定ネットワーク通信装置の識別子及び前記他ネットワーク通信装置の識別子に対応するコネクション識別子情報を前記通信管理テーブル内で検索し、対応するコネクション識別子情報が前記通信管理テーブル内に存在する場合に、前記特定ネットワーク通信装置と前記他ネットワーク通信装置との間に通信コネクションが確立したと判断するコネクション管理部を有することを特徴とする請求項１に記載の中継処理装置。

【請求項８】　前記第一の通信処理部は、所定の送信シーケンス番号が付与されたコネクション設定パケットを受信し、

前記通信管理テーブルは、前記第一の通信処理部により前記コネクション設定パケットが受信された場合に、受信された前記コネクション設定パケットの送信シーケンス番号に所定の値を加算した値を前記判断基準シーケンス番号として前記コネクション識別子情報に対応づけて記憶することを特徴とする請求項７に記載の中継処理装置。

【請求項９】　前記第二の通信処理部は、前記特定ネットワーク通信装置と前記他ネットワーク通信装置との間の通信コネクションの設定のために前記他ネットワーク通信装置より送信されたコネクション設定パケットを受信し、受信した前記コネクション設定パケットを前記第一の通信処理部に転送し、

前記第一の通信処理部は、前記第二の通信処理部より転送された前記コネクション設定パケットを前記特定ネットワーク通信装置へ送信するとともに、前記特定ネットワーク通信装置の識別子及び前記他ネットワーク通信装置の識別子を含み、前記コネクション設定パケットに対する応答として前記特定ネットワーク通信装置より送信された応答コネクション設定パケットを受信し、

前記中継処理装置は、更に、前記第一の通信処理部により前記応答コネクション設定パケットが受信された場合に、前記応答コネクション設定パケットに含まれた前記特定ネットワーク通信装置の識別子及び前記他ネットワーク通信装置の識別子をコネクション識別子情報として前記通信管理テーブルに登録するとともに、前記特定ネットワーク通信装置と前記他ネットワーク通信装置との間に通信コネクションが確立したと判断するコネクション管理部を有することを特徴とする請求項１に記載の中継処理装置。

【請求項１０】　前記コネクション管理部は、前記特定ネットワーク通信装置と前記他ネットワーク通信装置との間に通信コネクションが確立したと判断した場合に、前記通信管理テーブル内の対応するコネクション識別子情報にコネクション確立フラグを設定することを特徴とする請求項７又は９に記載の中継処理装置。

【請求項１１】　前記中継処理装置は、更に、一定周期ごとに前記通信管理テーブルを検査してコネクション識別子情報にコネクション確立フラグが設定されているか否かを確認し、コネクション確立フラグが設定されていないコネクション識別子情報を前記通信管理テーブルから削除するコネクション確認部を有することを特徴とする請求項１０に記載の中継処理装置。

【請求項１２】　前記第一の通信処理部は、所定の場合に、前記特定ネットワーク通信装置の識別子及び前記他ネットワーク通信装置の識別子を含み、前記特定ネットワーク通信装置と前記他ネットワーク通信装置との間の通信コネクションの切断のために前記特定ネットワーク通信装置より送信されたコネクション切断パケットを受信し、

前記コネクション管理部は、前記第一の通信処理部により前記コネクション切断パケットが受信された場合に、前記コネクション切断パケットに含まれた前記特定ネットワーク通信装置の識別子及び前記他ネットワーク通信装置の識別子に対応するコネクション識別子情報を前記通信管理テーブルから削除することを特徴とする請求項７又は９に記載の中継処理装置。

【請求項１３】　前記第一の通信処理部は、所定の場合に、前記特定ネットワーク通信装置の識別子及び前記他ネットワーク通信装置の識別子を含み、前記特定ネットワーク通信装置と前記他ネットワーク通信装置との間の

5

通信コネクションの強制切断のために前記特定ネットワーク通信装置より送信されたコネクション強制切断パケットを受信し、

前記コネクション管理部は、前記第一の通信処理部により前記コネクション強制切断パケットが受信された場合に、前記コネクション強制切断パケットに含まれた前記特定ネットワーク通信装置の識別子及び前記他ネットワーク通信装置の識別子に対応するコネクション識別子情報を前記通信管理テーブルから削除することを特徴とする請求項７又は９に記載の中継処理装置。

【請求項１４】　前記第二の通信処理部は、所定の場合に、前記特定ネットワーク通信装置の識別子及び前記他ネットワーク通信装置の識別子を含み、前記特定ネットワーク通信装置と前記他ネットワーク通信装置との間の通信コネクションの強制切断のために前記他ネットワーク通信装置より送信されたコネクション強制切断パケットを受信し、

前記コネクション管理部は、前記第二の通信処理部により前記コネクション強制切断パケットが受信された場合に、前記コネクション強制切断パケットに含まれた前記特定ネットワーク通信装置の識別子及び前記他ネットワーク通信装置の識別子に対応するコネクション識別子情報を前記通信管理テーブルから削除することを特徴とする請求項７又は９に記載の中継処理装置。

【請求項１５】　前記中継要否判断部は、ＴＣＰ（Ｔｒａｎｓｍｉｓｓｉｏｎ　Ｃｏｎｔｒｏｌ　Ｐｒｏｔｏｃｏｌ）プロトコルを用いるデータパケットについて中継処理の要否判断を行うことを特徴とする請求項１に記載の中継処理装置。

【請求項１６】　それぞれに少なくとも一つ以上の通信装置を有する複数のネットワークに接続された中継装置内で、前記複数のネットワークのうち特定のネットワークに関する中継処理を行う中継処理方法であって、

前記特定のネットワーク内の通信装置である特定ネットワーク通信装置から他のネットワーク内の通信装置である他ネットワーク通信装置に対して送信されたデータパケットであって、送信シーケンス番号として所定のシーケンス番号が付与されたデータパケットを順次受信する第一の通信処理ステップと、

データパケットに対する中継処理の要否判断の基準となるシーケンス番号を判断基準シーケンス番号として記憶する通信管理ステップと、

前記第一の通信処理ステップによりデータパケットが受信される度に、受信された受信データパケットの送信シーケンス番号と前記通信管理ステップにより記憶された判断基準シーケンス番号とを比較して前記受信データパケットについて中継処理の要否判断を行う中継要否判断ステップと、

前記中継要否判断ステップにより中継処理の対象とされた受信データパケットを前記他ネットワーク通信装置に対して送信する第二の通信処理ステップとを有することを特徴とする中継処理方法。

6

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】この発明は、ルータ装置に用いられるＴＣＰ（Ｔｒａｎｓｍｉｓｓｉｏｎ　Ｃｏｎｔｒｏｌ　Ｐｒｏｔｏｃｏｌ）プロトコルを使用したＩＰパケットの管理技術に関する。

【０００２】

【従来の技術】図１９は、例えば、特開平１１－２７３１７号公報に示された従来のルータである。図１９において、２００はＩＰルータ、２０１は中継判定処理手段、２０２は経路制御データベース手段、２０３はフラグメント識別用記憶領域、２０４～２０５はネットワークインタフェース、２０６～２０８はネットワーク、２０９～２１０はネットワークに接続した局、２１１は他のＩＰルータ、２２０～２２９は局が送出したフラグメントされたＩＰパケットである。

【０００３】このようなネットワークにおいて、局Ａ２０９が局Ｂ２１０に宛てて、ネットワークに１０個のフラグメントされたＩＰパケット２２０～２２９を送信した場合、従来のルータ２００では、ネットワークインタフェースＡ２０４によってフラグメントされたＩＰパケット２２０～２２９を受信すると、経路制御データベース手段２０２により、宛先アドレスである局Ｂ２１０がどのネットワークに属するかを調べ、中継判定処理手段２０１により、該当するネットワークインタフェースＢ２０５へ送出する。

【０００４】ルータ２００は、内部のバッファ不足等により、フラグメントされたＩＰパケット２２０～２２９を中継できない場合、中継判定処理手段２０１により、そのＩＰパケットのＩＰヘッダから、送信元ＩＰアドレス、宛先ＩＰアドレス、及び、ＩＤＥＮＴフィールド（このＩＤＥＮＴフィールドはＩＰパケットの各フラグメントの識別用として用いられる）の内容をフラグメント識別用記憶領域に保存して、ＩＰパケットを廃棄する。また、後続のフラグメントされたＩＰパケットが、フラグメント識別用記憶領域２０３に保存されている内容と一致する場合に、既に先行するＩＰパケットが廃棄されているので、中継する必要がないと判断して、そのＩＰパケットを廃棄する。

【０００５】

【発明が解決しようとする課題】上記のような従来のルータ２００では、フラグメントされたＩＰパケット内の一部のＩＰパケットを自身で廃棄した場合しか後続のフラグメントされたＩＰパケットを廃棄できないという問題がある。他のルータで、フラグメントされたＩＰパケット内の一部のＩＰパケットが廃棄された場合には自ルータはこの廃棄されたＩＰパケットを検出できない。そのため、後続する無効なデータを含むＩＰパケットがネ

ットワーク上を流れてしまい、ネットワーク全体の利用効率は十分に改善されない。

【０００６】この発明は、上述のような課題を解決するためになされたものであり、第一の目的は、トランスポート層にＴＣＰプロトコルを使用して通信されるユーザデータ（ＴＣＰセグメント）を管理する機能を実装することにより、データ抜けや重複による無効なトラフィックを検出して廃棄することにある。第二の目的は、無効なトラフィックの中継を削減することにより、ネットワークにおける輻輳を減らし、ネットワーク全体の利用効率を向上させることにある。

【０００７】

【課題を解決するための手段】本発明に係る中継処理装置は、それぞれに少なくとも一つ以上の通信装置を有する複数のネットワークに接続された中継装置内で、前記複数のネットワークのうち特定のネットワークに関する中継処理を行う中継処理装置であって、前記特定のネットワーク内の通信装置である特定ネットワーク通信装置から他のネットワーク内の通信装置である他ネットワーク通信装置に対して送信されたデータパケットであって、送信シーケンス番号として所定のシーケンス番号が付与されたデータパケットを順次受信する第一の通信処理部と、データパケットに対する中継処理の要否判断の基準となるシーケンス番号を判断基準シーケンス番号として記憶する通信管理テーブルと、前記第一の通信処理部によりデータパケットが受信される度に、受信された受信データパケットの送信シーケンス番号と前記通信管理テーブルに記憶された判断基準シーケンス番号とを比較して前記受信データパケットについて中継処理の要否判断を行う中継要否判断部と、前記中継要否判断部により中継処理の対象とされた受信データパケットを前記他ネットワーク通信装置に対して送信する第二の通信処理部とを有することを特徴とする。

【０００８】前記中継要否判断部は、受信データパケットを中継処理の対象とする度に、中継処理の対象とした受信データパケットの次に中継処理の対象となるデータパケットの送信シーケンス番号を次中継シーケンス番号として算出し、次中継シーケンス番号を算出する度に新たに算出した次中継シーケンス番号に更新しながら前記通信管理テーブルに次中継シーケンス番号を登録し、前記第二の通信処理部は、前記他ネットワーク通信装置がデータパケットを受信した場合に送達確認のために前記他ネットワーク通信装置から前記特定ネットワーク通信装置に対して送信された送達確認パケットであって、確認シーケンス番号として所定のシーケンス番号が付与された送達確認パケットを順次受信し、前記中継処理装置は、更に、前記第二の通信処理部により送達確認パケットが受信される度に新たに受信された送達確認パケットの確認シーケンス番号に更新しながら前記通信管理テーブルに確認シーケンス番号を登録する送達確認パケット管理部を有し、前記通信管理テーブルは、前記判断基準シーケンス番号として、前記中継要否判断部により最新に登録された次中継シーケンス番号と前記送達確認パケット管理部により最新に登録された確認シーケンス番号とを記憶し、前記中継要否判断部は、前記第一の通信処理部によりデータパケットが受信される度に、受信データパケットの送信シーケンス番号を、前記通信管理テーブルに記憶されている次中継シーケンス番号及び確認シーケンス番号のうち少なくともいずれか一つと比較して前記受信データパケットについて中継処理の要否判断を行うことを特徴とする。

【０００９】前記中継要否判断部は、前記第一の通信処理部によりデータパケットが受信される度に、受信データパケットの送信シーケンス番号と前記通信管理テーブルに記憶されている確認シーケンス番号とを比較し、前記受信データパケットの送信シーケンス番号の値が前記通信管理テーブルに記憶されている確認シーケンス番号の値以上である場合に、前記受信データパケットの送信シーケンス番号と前記通信管理テーブルに記憶されている次中継シーケンス番号とを比較し、前記受信データパケットの送信シーケンス番号の値が前記通信管理テーブルに記憶されている次中継シーケンス番号の値以下である場合に、前記受信データパケットを中継処理の対象とすることを特徴とする。

【００１０】前記中継要否判断部は、前記受信データパケットの送信シーケンス番号の値が前記通信管理テーブルに記憶されている確認シーケンス番号の値未満であった場合及び前記受信データパケットの送信シーケンス番号の値が前記通信管理テーブルに記憶されている次中継シーケンス番号の値よりも大きい場合に、前記受信データパケットの廃棄を決定することを特徴とする。

【００１１】前記中継要否判断部は、中継処理の対象となった中継対象データパケットの送信シーケンス番号に前記中継対象データパケットのデータサイズを加算した値を前記次中継シーケンス番号として算出し、前記第二の通信処理部は、前記他ネットワーク通信装置が受信した受信済データパケットの送信シーケンス番号に前記受信済データパケットのデータサイズを加算した値を前記確認シーケンス番号とする送達確認パケットを受信することを特徴とする。

【００１２】前記通信管理テーブルは、前記特定ネットワーク通信装置の識別子及び前記他ネットワーク通信装置の識別子をコネクション識別子情報として記憶しており、前記中継要否判断部により最新に登録された次中継シーケンス番号と前記送達確認パケット管理部により最新に登録された確認シーケンス番号とを前記コネクション識別子情報に対応づけて記憶し、前記第一の通信処理部は、前記特定ネットワーク通信装置の識別子及び前記他ネットワーク通信装置の識別子を含むデータパケットを順次受信し、前記中継要否判断部は、前記第一の通信

処理部によりデータパケットが受信される度に、受信データパケットに含まれた前記特定ネットワーク通信装置の識別子及び前記他ネットワーク通信装置の識別子に対応するコネクション識別子情報を前記通信管理テーブル内で検索し、検索したコネクション識別子情報に対応づけられた次中継シーケンス番号及び確認シーケンス番号のうち少なくともいずれか一つと前記受信データパケットの送信シーケンス番号とを比較して前記受信データパケットについて中継処理の要否判断を行うことを特徴とする。

【００１３】前記第一の通信処理部は、前記データパケットの受信に先立ち、前記特定ネットワーク通信装置の識別子及び前記他ネットワーク通信装置の識別子を含み、前記特定ネットワーク通信装置と前記他ネットワーク通信装置との間の通信コネクションの設定のために前記特定ネットワーク通信装置より送信されたコネクション設定パケットを受信し、前記通信管理テーブルは、前記第一の通信処理部により前記コネクション設定パケットが受信された場合に、受信された前記コネクション設定パケットに含まれた前記特定ネットワーク通信装置の識別子及び前記他ネットワーク通信装置の識別子をコネクション識別子情報として記憶し、前記第二の通信処理部は、前記コネクション設定パケットを前記他ネットワーク通信装置へ送信するとともに、前記特定ネットワーク通信装置の識別子及び前記他ネットワーク通信装置の識別子を含み、前記コネクション設定パケットに対する応答として前記他ネットワーク通信装置より送信された応答コネクション設定パケットを受信し、前記中継処理装置は、更に、前記第二の通信処理部により前記応答コネクション設定パケットが受信された場合に、前記応答コネクション設定パケットに含まれた前記特定ネットワーク通信装置の識別子及び前記他ネットワーク通信装置の識別子に対応するコネクション識別子情報を前記通信管理テーブル内で検索し、対応するコネクション識別子情報が前記通信管理テーブル内に存在する場合に、前記特定ネットワーク通信装置と前記他ネットワーク通信装置との間に通信コネクションが確立したと判断するコネクション管理部を有することを特徴とする。

【００１４】前記第一の通信処理部は、所定の送信シーケンス番号が付与されたコネクション設定パケットを受信し、前記通信管理テーブルは、前記第一の通信処理部により前記コネクション設定パケットが受信された場合に、受信された前記コネクション設定パケットの送信シーケンス番号に所定の値を加算した値を前記判断基準シーケンス番号として前記コネクション識別子情報に対応づけて記憶することを特徴とする。

【００１５】前記第二の通信処理部は、前記特定ネットワーク通信装置と前記他ネットワーク通信装置との間の通信コネクションの設定のために前記他ネットワーク通信装置より送信されたコネクション設定パケットを受信

し、受信した前記コネクション設定パケットを前記第一の通信処理部に転送し、前記第一の通信処理部は、前記第二の通信処理部より転送された前記コネクション設定パケットを前記特定ネットワーク通信装置へ送信するとともに、前記特定ネットワーク通信装置の識別子及び前記他ネットワーク通信装置の識別子を含み、前記コネクション設定パケットに対する応答として前記特定ネットワーク通信装置より送信された応答コネクション設定パケットを受信し、前記中継処理装置は、更に、前記第一の通信処理部により前記応答コネクション設定パケットが受信された場合に、前記応答コネクション設定パケットに含まれた前記特定ネットワーク通信装置の識別子及び前記他ネットワーク通信装置の識別子をコネクション識別子情報として前記通信管理テーブルに登録するとともに、前記特定ネットワーク通信装置と前記他ネットワーク通信装置との間に通信コネクションが確立したと判断するコネクション管理部を有することを特徴とする。

【００１６】前記コネクション管理部は、前記特定ネットワーク通信装置と前記他ネットワーク通信装置との間に通信コネクションが確立したと判断した場合に、前記通信管理テーブル内の対応するコネクション識別子情報にコネクション確立フラグを設定することを特徴とする。

【００１７】前記中継処理装置は、更に、一定周期ごとに前記通信管理テーブルを検査してコネクション識別子情報にコネクション確立フラグが設定されているか否かを確認し、コネクション確立フラグが設定されていないコネクション識別子情報を前記通信管理テーブルから削除するコネクション確認部を有することを特徴とする。

【００１８】前記第一の通信処理部は、所定の場合に、前記特定ネットワーク通信装置の識別子及び前記他ネットワーク通信装置の識別子を含み、前記特定ネットワーク通信装置と前記他ネットワーク通信装置との間の通信コネクションの切断のために前記特定ネットワーク通信装置より送信されたコネクション切断パケットを受信し、前記コネクション管理部は、前記第一の通信処理部により前記コネクション切断パケットが受信された場合に、前記コネクション切断パケットに含まれた前記特定ネットワーク通信装置の識別子及び前記他ネットワーク通信装置の識別子に対応するコネクション識別子情報を前記通信管理テーブルから削除することを特徴とする。

【００１９】前記第一の通信処理部は、所定の場合に、前記特定ネットワーク通信装置の識別子及び前記他ネットワーク通信装置の識別子を含み、前記特定ネットワーク通信装置と前記他ネットワーク通信装置との間の通信コネクションの強制切断のために前記特定ネットワーク通信装置より送信されたコネクション強制切断パケットを受信し、前記コネクション管理部は、前記第一の通信処理部により前記コネクション強制切断パケットが受信された場合に、前記コネクション強制切断パケットに含

まれた前記特定ネットワーク通信装置の識別子及び前記他ネットワーク通信装置の識別子に対応するコネクション識別子情報を前記通信管理テーブルから削除することを特徴とする。

【００２０】前記第二の通信処理部は、所定の場合に、前記特定ネットワーク通信装置の識別子及び前記他ネットワーク通信装置の識別子を含み、前記特定ネットワーク通信装置と前記他ネットワーク通信装置との間の通信コネクションの強制切断のために前記他ネットワーク通信装置より送信されたコネクション強制切断パケットを受信し、前記コネクション管理部は、前記第二の通信処理部により前記コネクション強制切断パケットが受信された場合に、前記コネクション強制切断パケットに含まれた前記特定ネットワーク通信装置の識別子及び前記他ネットワーク通信装置の識別子に対応するコネクション識別子情報を前記通信管理テーブルから削除することを特徴とする。

【００２１】前記中継要否判断部は、ＴＣＰ（Ｔｒａｎｓｍｉｓｓｉｏｎ ＣｏｎｔｒｏｌＰｒｏｔｏｃｏｌ）プロトコルを用いるデータパケットについて中継処理の要否判断を行うことを特徴とする。

【００２２】本発明に係る中継処理方法は、それぞれに少なくとも一つ以上の通信装置を有する複数のネットワークに接続された中継装置内で、前記複数のネットワークのうち特定のネットワークに関する中継処理を行う中継処理方法であって、前記特定のネットワーク内の通信装置である特定ネットワーク通信装置から他のネットワーク内の通信装置である他ネットワーク通信装置に対して送信されたデータパケットであって、送信シーケンス番号として所定のシーケンス番号が付与されたデータパケットを順次受信する第一の通信処理ステップと、データパケットに対する中継処理の要否判断の基準となるシーケンス番号を判断基準シーケンス番号として記憶する通信管理ステップと、前記第一の通信処理ステップによりデータパケットが受信される度に、受信された受信データパケットの送信シーケンス番号と前記通信管理ステップにより記憶された判断基準シーケンス番号とを比較して前記受信データパケットについて中継処理の要否判断を行う中継要否判断ステップと、前記中継要否判断ステップにより中継処理の対象とされた受信データパケットを前記他ネットワーク通信装置に対して送信する第二の通信処理ステップとを有することを特徴とする。

【００２３】

【発明の実施の形態】実施の形態１．実施の形態１～６では、本発明に係る中継処理装置の例としてラインカードを用いる場合について説明する。図１は、ラインカードを複数枚実装したＩＰルータ１０の構成を示し、図２は各ラインカードの内部構成を示している。なお、ＩＰルータ１０は中継装置に相当する。

【００２４】図１に示すように、ＩＰルータ１０は、１

枚の制御カード１１と、複数枚のラインカード１から構成される。実施の形態１では、ラインカード１を４枚実装した場合の構成例であり、ＩＰルータ１０内のラインカード１Ａ～１Ｄは、それぞれＬＡＮ１２、ＬＡＮ１３、ＷＡＮ１４、ＷＡＮ１５と接続されている。ラインカードＡ１ＡはＬＡＮ１２に関する中継処理を、ラインカードＢ１ＢはＬＡＮ１３に関する中継処理を、ラインカードＣ１ＣはＷＡＮ１４に関する中継処理を、ラインカードＤ１ＤはＷＡＮ１５に関する中継処理を、それぞれ行う。また、各ラインカードにとって、自己に接続するネットワークは特定のネットワークに相当し、他のラインカードに接続するネットワークは他のネットワークに相当する。例えば、ラインカードＡ１Ａにとっては、ＬＡＮ１２は特定のネットワークであり、ＬＡＮ１３は他のネットワークに相当する。また、特定のネットワーク内の通信装置は特定ネットワーク通信装置に相当し、他のネットワーク内の通信装置は他ネットワーク通信装置に相当する。例えば、ラインカードＡ１Ａにとっては、ＬＡＮ１２に接続されたクライアント１８（端末Ａ）は特定ネットワーク通信装置であり、ＬＡＮ１３に接続されたサーバ１９（端末Ｂ）は他ネットワーク通信装置である。制御カード１１とすべてのラインカード１Ａ～１Ｄは、制御バス１６で接続される。また、ラインカード１Ａ～１Ｄ同士、及び、制御カード１１と各ラインカード１Ａ～１Ｄは、それぞれデータバス１７で接続される。ＩＰルータ１０では、１０組のデータバス１７を有する。

【００２５】次に、図２を参照してラインカードの構成を説明する。入力側ＴＣＰセグメント管理部２は、ＬＡＮ１２～１３またはＷＡＮ１４～１５から受信したＩＰパケットの内、トランスポート層にＴＣＰプロトコルを使用するＩＰパケットを受けて、ＴＣＰ管理テーブル４の制御、及び、重複やデータ抜けが発生したＩＰパケットの廃棄を行う。なお、後述するように、入力側ＴＣＰセグメント管理部２には、中継要否判断部に相当する要素が含まれる。出力側ＴＣＰセグメント管理部３は、ＬＡＮ１２～１３またはＷＡＮ１４～１５へ送出するＩＰパケットの内、トランスポート層にＴＣＰプロトコルを使用するＩＰパケットを受けて、ＴＣＰ管理テーブル４の制御を行う。ＴＣＰ管理テーブル４には、入力側ＴＣＰセグメント管理部２による中継処理の要否判断に用いるシーケンス番号（判断基準シーケンス番号）が記憶されている。ＴＣＰ管理テーブルは通信管理テーブルに相当する。

【００２６】入力フレーム種別判定部５は、レイヤ２／３処理部８から渡されたＩＰパケットのトランスポート層のプロトコル種別を判別して、トランスポート層にＴＣＰプロトコルを使用するＩＰパケットを入力側ＴＣＰセグメント管理部２に渡し、ＴＣＰプロトコル以外のプロトコルであればそのまま中継する。出力フレーム種別

判定部６は、他のラインカードから中継されたＩＰパケットのトランスポート層のプロトコル種別を判別して、トランスポート層にＴＣＰプロトコルを使用するＩＰパケットを出力側ＴＣＰセグメント管理部３に渡し、ＴＣＰプロトコル以外のプロトコルであればそのままレイヤ２／３処理部８に渡す。

【００２７】ネットワーク送受信回路７は、ＬＡＮ１２～１３またはＷＡＮ１４～１５上の隣接ルータまたは端末との間で、ＩＰフレームを送受信する。ネットワーク送受信回路７は、第一の通信処理部に相当する。レイヤ２／３処理部８は、ＬＡＮ１２～１３またはＷＡＮ１４～１５から受信したＩＰフレームをデフレーム化して、ＩＰプロトコル処理を行う。また、レイヤ２／３処理部８は、ＬＡＮ１２～１３またはＷＡＮ１４～１５に送出するためにフレーム化を行う。カード間送受信回路９は、制御カード１１または他のラインカードとの間で、データバス１７を経由して、ＩＰパケット２０を送受信する。カード間送受信回路９は、第二の通信処理部に相当する。

【００２８】図１において、端末Ａと端末Ｂ間において、ＴＣＰプロトコル通信を行う場合を例とする。この時、端末Ａをクライアント１８、端末Ｂをサーバ１９とする。

【００２９】図３に、入力側ＴＣＰセグメント管理部２と出力側ＴＣＰセグメント管理部３で処理する、トランスポート層にＴＣＰプロトコルを使用するＩＰパケット２０の形式を示す。また、図４に、ＩＰパケット２０内のフラグビット３２の詳細を示す。

【００３０】ＩＰパケット２０は、ネットワーク層のＩＰヘッダ２１、トランスポート層のＴＣＰヘッダ２２、ユーザデータ２３の順で構成される。また、ＴＣＰプロトコルにおいて、ＴＣＰヘッダ２２とユーザデータ２３を合わせて、ＴＣＰセグメント２４と称する。

【００３１】ＩＰヘッダ２１は、プロトコル番号２５、送信元ＩＰアドレス２６、及び、送信先ＩＰアドレス２７などから構成される。プロトコル番号２５は、ＩＰパケット２０が運ぶ上位のプロトコルを示す識別番号であり、６であればＴＣＰ（トランスミッションコントロール）プロトコルを、１７であればＵＤＰ（ユーザデータグラム）プロトコルを示す。ＴＣＰセグメント２４の場合は、６に設定されている。送信元ＩＰアドレス２６は、送信元を示す識別番号である。送信先ＩＰアドレス２７は、送信先を示す識別番号である。送信元ＩＰアドレス２６と送信先ＩＰアドレス２７は、ＩＰプロトコルのバージョンによってサイズが異なり、ＩＰｖ４では３２ビット、ＩＰｖ６では１２８ビットで表される。

【００３２】ＴＣＰヘッダ２２は、送信元ポート番号２８、送信先ポート番号２９、シーケンス番号３０、確認応答番号３１、及び、フラグビット３２などから構成される。送信元ポート番号２８は、送り元のポートの識別

番号である。送信先ポート番号２９は、送り先のポートの識別番号である。送信元ポート番号２８と送信先ポート番号２９は、１６ビットで表される。シーケンス番号３０は、ＳＹＮビット３４がＯＮの場合に、接続時のシーケンス番号３０の初期値を指定する。それ以外の場合は、このＴＣＰセグメント２４内のユーザデータ２３が送信データ列中のどの位置にあるかを示す。このシーケンス番号３０は、送信シーケンス番号に相当する。確認応答番号３１は、ＡＣＫビット３６がＯＮの時のみ有効であり、次に受信を期待するシーケンス番号３０を指定する。この確認応答番号３１未満のシーケンス番号３０を持つユーザデータ２３は受信側で正常に受信されたことを示す。この確認応答番号３１は、確認シーケンス番号に相当する。

【００３３】フラグビット３２は、ＴＣＰコネクション接続／切断、送達確認などのＴＣＰセグメント２４の種類を示す。フラグビット３２には、ＦＩＮビット３３、ＳＹＮビット３４、ＲＳＴビット３５、ＡＣＫビット３６などが存在する。本明細書では、１の場合をＯＮ、０の場合をＯＦＦと記述する。

【００３４】ＦＩＮビット３３は、ＯＮの場合に、このＴＣＰセグメント２４の送り元からこれ以上送るユーザデータ２３がないため、送り元はＴＣＰコネクションを切断しようとしていることを示す。しかし、この状態では相手からのＴＣＰセグメント２４は受信可能である。この状態で、相手からＦＩＮビット３３がＯＮのセグメントを受信した時点で、ＴＣＰコネクションは削除される。ＳＹＮビット３４は、ＯＮの場合に、シーケンス番号３０に初期値が設定されていることを示す。これは、ＴＣＰコネクション確立時に使用される。ＲＳＴビット３５は、ＯＮの場合に、このＴＣＰセグメント２４を送信した端末から、一方的かつ強制的にＴＣＰコネクションを切断することを意味する。これは、再送信などの通常の方法で回復できないエラーが発生した場合などに使用される。通常、ＴＣＰセグメント２４は、ＦＩＮビット３３、ＳＹＮビット３４、ＲＳＴビット３５の内、最大でも１個のビットのみＯＮになる。

【００３５】ＡＣＫビット３６は、ＯＮの場合に確認応答番号３１が有効であることを示し、このＴＣＰセグメント２４に送達確認の情報を含むことを示す。

【００３６】図５にＴＣＰ管理テーブル４を示す。このＴＣＰ管理テーブル４は、単一方向のＴＣＰコネクション毎に、コネクション識別子４１、Ｓｅｑ番号４２、Ａｃｋ番号４３、及び、確立フラグ４４を管理する。本明細書では、コネクション識別子４１、Ｓｅｑ番号４２、及び、Ａｃｋ番号４３を一組として、コネクション情報と称する。コネクション情報は、単一方向のＴＣＰコネクション毎に存在する。

【００３７】コネクション識別子４１は、送信元ＩＤ４５と送信先ＩＤ４６を組合わせたものである。送信元Ｉ

Ｄ４５は、送信元のＴＣＰソケットを示し、送信元ポート番号２８と送信元ＩＰアドレス２６を組合わせたものである。送信先ＩＤ４６は、送信先のＴＣＰソケットを示し、送信先ポート番号２９と送信先ＩＰアドレス２７を組合わせたものである。送信元ＩＤ４５と送信先ＩＤ４６は、ＩＰプロトコルのバージョンによってサイズが異なり、ＩＰｖ４では４８ビット、ＩＰｖ６では１４４ビットで表される。そのため、コネクション識別子４１は、ＩＰｖ４では９６ビット、ＩＰｖ６では２８８ビットで表される。

【００３８】Ｓｅｑ番号４２は、コネクション識別子４１毎に、ラインカード１が次に受信するＴＣＰセグメント２４のシーケンス番号３０を示す。なお、Ｓｅｑ番号４２は、次中継シーケンス番号に相当する。Ａｃｋ番号４３は、コネクション識別子４１毎に、ラインカード１が受信した最新の送達確認用ＴＣＰセグメント２４の確認応答番号３１を示す。なお、Ａｃｋ番号４３は確認シーケンス番号に相当する。また、次中継シーケンス番号（Ｓｅｑ番号４２）及び、確認シーケンス番号（Ａｃｋ番号４３）をあわせて判断基準シーケンス番号とする。確立フラグ（コネクション確立フラグ）４４は、ＴＣＰプロトコルで通信する端末間で、双方向のＴＣＰコネクションが確立した場合にＯＮに設定する。単方向のＴＣＰコネクションが確立した時点ではＯＦＦに設定する。また、一定周期で確立フラグ４４を監視する際に、ＯＦＦであった場合はＣＨＥＣＫに変更する。

【００３９】このように、ＴＣＰ管理テーブル４で、単一方向のＴＣＰコネクション毎に、ラインカード１が次に受信するＴＣＰセグメント２４のシーケンス番号３０を管理することで、データの抜けを検出することができる。また、ＴＣＰ管理テーブル４で、単一方向のＴＣＰコネクション毎に、ラインカード１が受信した最新の送達確認用のＴＣＰセグメント２４の確認応答番号３１を管理することで、ＴＣＰプロトコル通信における受信側が受け取り済みのＴＣＰセグメント２４を把握し、データの重複を検出することができる。また、本発明は、ＩＰルータ１０の個々のラインカード１に実装される機能であり、他のルータ装置の影響を受けない／与えないため、他社のルータ装置との相互接続性を保証することができる。

【００４０】図６は、入力側ＴＣＰセグメント管理部２の詳細を示したものである。なお、図１と同等の機能を有する箇所には同一番号を付し説明を省略する。

【００４１】入力側フラグビット判定部５１は、ＩＰパケット２０内のフラグビット３２を確認する。ＴＣＰコネクション確立の場合は、ＩＰパケット２０を入力側コネクション情報管理部５４に渡す。なお、ＴＣＰコネクション確立の場合とは、ＴＣＰセグメント２４のＳＹＮビット３４がＯＮであり、かつ、ＦＩＮビット３３、ＲＳＴビット３５がＯＦＦである場合を指す。ＴＣＰコネクション切断の場合は、ＩＰパケット２０を入力側コネクション情報管理部５４に渡す。なお、ＴＣＰコネクション切断の場合とは、ＴＣＰセグメント２４のＳＹＮビット３４がＯＦＦであり、かつ、ＦＩＮビット３３、または、ＲＳＴビット３５のいずれかがＯＮである場合を指す。データ送信の場合は、ＩＰパケット２０をフィルタ部５２に渡す。なお、データ送信の場合とは、ＴＣＰセグメント２４のＦＩＮビット３３、ＳＹＮビット３４、ＲＳＴビット３５、ＡＣＫビット３６のすべてがＯＦＦである場合を指す。送達確認の場合は、カード間送受信回路９を経由して、他のラインカードに転送する。なお、送達確認の場合とは、ＴＣＰセグメント２４のＦＩＮビット３３、ＳＹＮビット３４、ＲＳＴビット３５のすべてがＯＦＦであり、かつ、ＡＣＫビット３６がＯＮである場合を指す。

【００４２】フィルタ部５２は、データ送信の場合に、入力側フラグビット判定部５１から渡されたＴＣＰセグメント２４に関して、ＴＣＰ管理テーブル４を参照して、ＴＣＰセグメント２４の正当性（連続するデータ列であること）を確認し、中継処理の要否判断を行なう。Ｓｅｑ番号更新部５３は、データ送信の場合に、ＴＣＰ管理テーブル４の該当するコネクション情報のＳｅｑ番号４２の現在の値に、ＴＣＰセグメント２４のデータサイズを加算し、次に受信する（次に中継処理の対象となる）ＴＣＰセグメント２４のシーケンス番号３０（次中継シーケンス番号）を算出する。また、コネクション情報のＳｅｑ番号４２を、その算出値に更新する。フィルタ部５２及びＳｅｑ番号更新部５３は、中継要否判断部に相当する。入力側コネクション情報管理部５４は、コネクション確立／切断時に、ＴＣＰセグメント２４からコネクション情報を生成して、ＴＣＰ管理テーブル４に登録、または、ＴＣＰ管理テーブル４から削除する。入力側コネクション情報管理部５４は、後述する出力側コネクション情報管理部６３とともに、コネクション管理部に相当する。

【００４３】コネクション確認部５５は、一定周期でＴＣＰ管理テーブル４の確立フラグ４４を監視し、２周期分（一定周期をＴとした場合は２Ｔ）を経過しても、確立フラグ４４がＯＮでない場合、そのコネクション情報をＴＣＰ管理テーブル４から削除する。

【００４４】図７は、出力側ＴＣＰセグメント管理部３の詳細を示したものである。なお、図１と同等の機能を有する箇所には同一番号を付し説明を省略する。

【００４５】出力側フラグビット判定部６１は、ＩＰパケット２０内のフラグビット３２を確認する。ＴＣＰコネクション確立の場合は、ＩＰパケット２０を出力側コネクション情報管理部６３に渡す。ＴＣＰコネクション切断の場合は、ＩＰパケット２０を出力側コネクション情報管理部６３に渡す。送達確認の場合は、ＩＰパケット２０をＡｃｋ番号更新部６２に渡す。それ以外の場合

は、レイヤ２／３処理部８、及び、ネットワーク送受信回路７を経由して、他のラインカードに転送する。それ以外の場合とは、データ送信時が該当する。

【００４６】Ａｃｋ番号更新部６２は、送達確認の場合に、ＴＣＰセグメント２４の確認応答番号３１を、ＴＣＰ管理テーブル４の該当するコネクション情報のＡｃｋ番号４３に更新する。なお、Ａｃｋ番号更新部６２は、送達確認パケット管理部に相当する。出力側コネクション情報管理部６３は、コネクション確立時に、ＴＣＰセグメント２４からコネクション情報を生成して、ＴＣＰ管理テーブル４に登録する。また、コネクション情報が既にＴＣＰ管理テーブル４に登録されており、かつ、対応する確立フラグ４４がＯＮでない場合は、ＯＮに設定する。なお、出力側コネクション情報管理部６３は、前述の入力側コネクション情報管理部５４とともにコネクション管理部に相当する。

【００４７】このように、入力側ＴＣＰセグメント管理部２において、ＴＣＰ管理テーブル４でコネクション情報のＳｅｑ番号４２を管理して、ラインカード１が次に受信するＴＣＰセグメント２４を予測することにより、データ抜けによる無効なトラフィックを削減することができる。これについては後述する。また、出力側ＴＣＰセグメント管理部３において、ＴＣＰ管理テーブル４でコネクション情報のＡｃｋ番号４３を管理して、ＴＣＰプロトコル通信における受信側が受け取り済みのＴＣＰセグメント２４を把握することにより、入力側ＴＣＰセグメント管理部２でデータ重複による無効なトラフィックを削減することができる。これについては後述する。

【００４８】実施の形態２．本実施の形態では、実施の形態１で示したラインカード１の処理のうち、コネクション確立時の処理の詳細を説明する。

【００４９】ＴＣＰコネクションを確立するために、ＴＣＰプロトコルで通信する端末間で、３ウェイハンドシェークと呼ばれる手順を行う。ＴＣＰコネクション確立を要求するためのＴＣＰセグメント２４は、ＳＹＮビット３４がＯＮに設定されている。本明細書では、このＴＣＰセグメント２４を、ＳＹＮセグメント（コネクション設定パケット）と称する。また、送達確認用のＴＣＰセグメント２４は、ＡＣＫビット３６がＯＮに、かつ、ＦＩＮビット３３とＲＳＴビット３５がＯＦＦに設定されている。本明細書では、このＴＣＰセグメント２４を送達確認セグメント（送達確認パケット）と称する。

【００５０】３ウェイハンドシェークの動作を図８を用いて説明する。なお、図８において、記述のないＦＩＮビット３３、ＳＹＮビット３４、ＲＳＴビット３５、ＡＣＫビット３６は、ＯＦＦに設定されていることを意味する。

【００５１】まず、第一フェーズとして、クライアント１８は、接続したいサーバ１９のポート番号と、クライアント１８の初期シーケンス番号を指定したＳＹＮセグメント７１を、サーバ１９に対して送信する。このＳＹＮセグメント７１は、フラグビット３２の内、ＳＹＮビット３４のみがＯＮに設定されている。

【００５２】次に、第二フェーズとして、サーバ１９は、サーバ１９側の初期シーケンス番号を指定したＳＹＮセグメント７２を、クライアント１８に対して送信する。このＳＹＮセグメント７２は、フラグビット３２の内、ＳＹＮビット３４とＡＣＫビット３６のみがＯＮに設定されている。また、確認応答番号３１には、クライアント１８からのＳＹＮセグメント７１のシーケンス番号３０に１を加算した値が設定される。なお、第二フェーズのＳＹＮセグメントは、第一フェーズのＳＹＮセグメントに対応する応答として送信されており、応答コネクション設定パケットに相当する。

【００５３】最後に、第三フェーズとして、クライアント１８は、サーバ１９からのＳＹＮセグメント７２に対して、送達確認のＴＣＰセグメント７３で応答する。このＴＣＰセグメント７３は、フラグビット３２の内、ＡＣＫビット３６のみがＯＮに設定されている。また、確認応答番号３１には、サーバ１９からのＳＹＮセグメント７２のシーケンス番号３０に１を加算した値が設定される。

【００５４】ラインカード１では、ＴＣＰコネクションを確立するためのＳＹＮセグメントの受信を起因として、ＴＣＰ管理テーブル４に、コネクション情報を登録する。この処理は、ＳＹＮセグメントを発行した端末の種類（クライアント１８、または、サーバ１９）により、２種類の方法に分けられる。端末の種類は、フラグビット３２のＡＣＫビット３６の設定値から判断する。ＡＣＫビット３６がＯＦＦであるＳＹＮセグメント７１の発行元はクライアント１８、ＡＣＫビット３６がＯＮであるＳＹＮセグメント７２の発行元はサーバ１９である。

【００５５】実施の形態２では、クライアント１８からのＳＹＮセグメント７１の受信を起因とした、コネクション情報の登録について説明する。つまり、本実施の形態では、クライアント１８からのＳＹＮセグメントを受信した場合のラインカードＡ１Ａの処理について説明する。

【００５６】この場合は、コネクション情報が有効になるまでに、２段階の処理を行う。第一段階で、３ウェイハンドシェークの第一フェーズのＳＹＮセグメント７１に基づき、ＴＣＰ管理テーブル４にコネクション情報を登録する。この時、確立フラグ４４はＯＦＦのままとする。第二段階で、３ウェイハンドシェークの第二フェーズのＳＹＮセグメント７２を受けた時点で、第一段階で登録したコネクション情報に対応する確立フラグ４４をＯＮにする。ラインカードＡ１Ａでは、第一段階を入力側ＴＣＰセグメント管理部２で処理し、第二段階を出力側ＴＣＰセグメント管理部３で行う。

【００５７】図９は、ＴＣＰコネクション確立の内、ＳＹＮセグメントによるコネクション情報の登録処理のフローチャートである。この図９は、実施の形態２の第一段階の処理である。但し、図９のフローチャートでは、ステップ９１～ステップ９３を除き、クライアント１８からのＳＹＮセグメント７１と、サーバ１９からのＳＹＮセグメント７２で同一処理を行う。そのため、図９の各ステップの説明では、ＳＹＮセグメント７１とＳＹＮセグメント７２に共通な場合はＳＹＮセグメントとして記述する。

【００５８】入力側フラグビット判定部５１は、ＴＣＰセグメント２４からフラグビット３２を抽出（ステップ８１）し、ＳＹＮビット３４の設定値から、ＴＣＰコネクション確立を要求するためのＳＹＮセグメントであるか否かを判定する（ステップ８２）。ＳＹＮビット３４がＯＮの場合はステップ８３に進む。また、ＳＹＮビット３４がＯＦＦの場合は終了する。但し、入力側フラグビット判定部５１に渡されたＩＰパケットは、４種類（ＴＣＰコネクション確立、ＴＣＰコネクション切断、データ送信、送達確認）のいずれかに必ず該当するため、ここで示す終了とは、他の条件（ＴＣＰコネクション切断、データ送信、送達確認）の判定に進むことを意味する。実施の形態２では、クライアントからのＳＹＮセグメント７１は、ＳＹＮビットがＯＮであるため、ステップ８３に進む。

【００５９】ステップ８２でＹｅｓの場合は、入力側コネクション情報管理部５４は、ＩＰパケット２０内の、送信元ＩＰアドレス２６、送信元ポート番号２８、送信先ＩＰアドレス２７、送信先ポート番号２９を組合わせて、コネクション識別子４１を生成する（ステップ８３）。次に、生成したコネクション識別子４１をキーとして、ＴＣＰ管理テーブル４を検索（ステップ８４）し、一致するコネクション識別子が既に登録されているか否かを確認する（ステップ８５）。既にＴＣＰ管理テーブル４に登録されている場合は、新しい情報に更新するために、ステップ８４で検出した情報（旧情報）をＴＣＰ管理テーブル４から削除する（ステップ８６）。

【００６０】既にＴＣＰ管理テーブル４に登録されているケースとしては、図８において、クライアント１８がサーバ１９にＴＣＰコネクション確立を要求した際に、サーバ１９が停止している場合がある。この時、クライアント１８は、サーバ１９からの応答がないため、コネクション確立タイムアウトにより、ＳＹＮセグメント７１を再送することになる。

【００６１】入力側コネクション情報管理部５４は、まず、ＴＣＰ管理テーブル４の空きエントリに、ステップ８３で生成したコネクション識別子４１を登録する（ステップ８７）。次に、ＳＹＮセグメントからシーケンス番号３０を抽出する（ステップ８８）。なお、ＳＹＮセグメントにおけるシーケンス番号３０は、送信先ＩＤ４６で示される端末が、送信元ＩＤ４５で示される端末のポートに送信するＴＣＰセグメントにシーケンシャルに付与する番号の初期値になる。そして、シーケンス番号３０に１を加算した値を、ステップ８７で登録したコネクション識別子４１に対応するＳｅｑ番号４２に登録する（ステップ８９）。また、シーケンス番号３０の値を、ステップ８７で登録したコネクション識別子４１に対応するＡｃｋ番号４３に登録する（ステップ９０）。

【００６２】入力側コネクション情報管理部５４は、最後に、ＴＣＰセグメント２４のＡＣＫビット３６の設定値を確認（ステップ９１）し、ステップ８７で登録したコネクション識別子４１に対応する確立フラグ４４を設定する。ＡＣＫビット３６がＯＦＦの場合は、確立フラグ４４をＯＦＦに設定する（ステップ９２）。また、ＡＣＫビット３６がＯＮの場合は、確立フラグ４４をＯＮに設定する（ステップ９３）。実施の形態２では、クライアント１８からのＳＹＮセグメント７１は、ＡＣＫビット３６がＯＦＦであるため、確立フラグ４４をＯＦＦに設定する。

【００６３】最後に、入力側コネクション情報管理部５４で処理されたＩＰパケット２０は、カード間送受信回路９を経由して、そのＩＰパケット２０を送出すべきラインカード１Ｂ～１Ｄに転送される。

【００６４】図１０は、サーバ１９からの第二フェーズのＳＹＮセグメント７２による、コネクション情報の有効化処理のフローチャートである。この図は、実施の形態２の第二段階の処理である。

【００６５】出力側フラグビット判定部６１は、ＴＣＰセグメント２４からフラグビット３２を抽出（ステップ１０１）し、ＳＹＮビット３４の設定値から、ＳＹＮセグメントであるか否かを判定する（ステップ１０２）。ＳＹＮビット３４がＯＮの場合はステップ１０３に進む。また、ＳＹＮビット３４がＯＦＦの場合は終了する。但し、出力側フラグビット判定部６１に渡されたＩＰパケットは、４種類（ＴＣＰコネクション確立、ＴＣＰコネクション切断、データ送信、送達確認）のいずれかに必ず該当するため、ここで示す終了とは、他の条件（ＴＣＰコネクション切断、データ送信、送達確認）の判定に進むことを意味する。実施の形態２では、サーバ１９からの第二フェーズのＳＹＮセグメント７２は、ＳＹＮビット３４がＯＮであるため、ステップ１０３に進む。

【００６６】出力側コネクション情報管理部６３は、ＩＰパケット２０内の、送信先ＩＰアドレス２７、送信先ポート番号２９を組合わせて、送信元ＩＤ４５を生成する（ステップ１０３）。また、ＩＰパケット２０内の、送信元ＩＰアドレス２６、送信元ポート番号２８を組合わせて、送信先ＩＤ４６を生成する（ステップ１０４）。そして、ステップ１０３で生成した送信元ＩＤ４５と、ステップ１０４で生成した送信先ＩＤ４６を組合

わせて、コネクション識別子４１を算出する（ステップ１０５）。出力側コネクション情報管理部６３では、入力側コネクション情報管理部５４と異なり、ＩＰパケット２０内の送信元／送信先を反転して、コネクション識別子４１を生成する。次に、生成したコネクション識別子４１をキーとして、ＴＣＰ管理テーブル４を検索（ステップ１０６）し、既に登録されているか否かを確認する（ステップ１０７）。登録されている場合はステップ１０８に進み、登録されていない場合はステップ１０９に進む。

【００６７】ステップ１０７でＹｅｓの場合は、出力側コネクション情報管理部６３は、ステップ１０６で検出したコネクション識別子４１に対応する確立フラグ４４をＯＮに設定する（ステップ１０８）。この時点で、コネクション情報は有効になる。

【００６８】最後に、出力側コネクション情報管理部６３で処理されたＩＰパケット２０は、レイヤ２／３処理部８に渡される（ステップ１０９）。

【００６９】なお、図８とは逆の場合、すなわち、第一フェーズのＳＹＮセグメントがサーバ１９からクライアント１８に対して送信され、第二フェーズのＳＹＮセグメントがクライアント１８からサーバ１９に対して送信された場合は、第一段階において、ラインカードＢ１Ｂの入力側ＴＣＰセグメント管理部２がＴＣＰ管理テーブル４にコネクション情報を登録し、第二段階において、出力側ＴＣＰセグメント管理部３が第一段階で登録したコネクション情報に対応する確立フラグ４４をＯＮにする。

【００７０】ＴＣＰプロトコル通信では、各端末はＴＣＰセグメント２４に付与するシーケンス番号３０をそれぞれ別々に管理するため、ＴＣＰ管理テーブル４を使用して、データ抜けやデータ重複による無効なトラフィックを検出するためには、単一方向のＴＣＰコネクション単位で管理する必要がある。ラインカード１において、３ウェイハンドシェークの第一フェーズのＳＹＮセグメント７１の受信を起因として、ＴＣＰ管理テーブル４にコネクション情報を登録することにより、クライアント１８からサーバ１９への方向に関して、ＴＣＰコネクション単位で管理することができる。

【００７１】実施の形態２では、コネクション情報の登録と有効化を別のフェーズで行うため、有効でないコネクション情報がＴＣＰ管理テーブル４に登録される場合がある。例えば、前述した、図８において、クライアント１８がサーバ１９にＴＣＰコネクション確立を要求した際に、サーバ１９が停止している場合がある。この時、クライアント１８は、ＳＹＮセグメント７１を再送することになるが、無限に繰り返すのではなく、一定期間を超えた場合にはＳＹＮセグメント７１を再送するのを停止する。

【００７２】このようなＴＣＰ管理テーブル４のリソースの浪費を防止するため、コネクション確認部５５は、一定周期で、ＴＣＰ管理テーブル４に登録されているすべてのコネクション情報の確立フラグ４４を監視し、無効のコネクション情報を削除する。

【００７３】図１１は、コネクション情報の監視処理のフローチャートである。

【００７４】コネクション確認部５５は、一定周期ごとに起動し、ＴＣＰ管理テーブル４の確立フラグ４４を確認（ステップ１１１）し、確立フラグ４４の値により分岐する（ステップ１１２）。確立フラグ４４がＯＮの場合は、ステップ１１５に進む。確立フラグ４４がＯＦＦの場合は、確立フラグ４４をＣＨＥＣＫに設定する（ステップ１１３）。確立フラグ４４がＣＨＥＣＫの場合は、該当するコネクション情報をＴＣＰ管理テーブル４から削除する（ステップ１１４）。その時点でＴＣＰ管理テーブル４に登録されているすべてのコネクション情報に対して、ステップ１１１～ステップ１１４の処理を行われるまで繰り返す（ステップ１１５）。

【００７５】このように、定期的にＴＣＰ管理テーブル４に登録されているコネクション情報を監視し、無効であるコネクション情報を検出して削除することにより、ＴＣＰ管理テーブル４のリソースの浪費を防止することができる。

【００７６】実施の形態３．実施の形態３では、サーバ１９からの第二フェーズのＳＹＮセグメント７２の受信を起因とした、コネクション情報の登録について説明する。この場合は、コネクション情報が有効になるまでに、１段階の処理を行う。この場合、３ウェイハンドシェークの第二フェーズのＳＹＮセグメント７２を受けた時点で、そのＳＹＮセグメント７２に基づき、ＴＣＰ管理テーブル４にコネクション情報を登録すると同時に、そのコネクション情報に対応する確立フラグ４４をＯＮにする。

【００７７】サーバ１９からの第二フェーズのＳＹＮセグメント７２によるコネクション情報の登録処理は、ラインカードＢ１Ｂの入力側ＴＣＰセグメント管理部２で行う。フローチャートは図９と同様である。

【００７８】実施の形態２との違いは、ＡＣＫビット３６の値により、ＴＣＰ管理テーブル４の確立フラグ４４への設定値が異なることである。ステップ９２～ステップ９３のいずれを選択するかにある。実施の形態３では、サーバ１９からのＳＹＮセグメント７２は、ＡＣＫビット３６がＯＮであるため、ステップ９３に進み、確立フラグ４４をＯＮに設定する。

【００７９】なお、図８とは逆の場合、すなわち、第一フェーズのＳＹＮセグメントがサーバ１９からクライアント１８に対して送信され、第二フェーズのＳＹＮセグメントがクライアント１８からサーバ１９に対して送信された場合は、ラインカードＡ１Ａの入力側ＴＣＰセグメント管理部２がコネクション情報の登録処理を行い、

確立フラグをＯＮにする。

【００８０】前述したが、ＴＣＰプロトコル通信では、各端末はＴＣＰセグメント２４に付与するシーケンス番号３０をそれぞれ別々に管理するため、ＴＣＰ管理テーブル４を使用して、データ抜けやデータ重複による無効なトラフィックを検出するためには、単一方向のＴＣＰコネクション単位で管理する必要がある。ラインカード１において、３ウェイハンドシェークの第二フェーズのＳＹＮセグメント７２の受信を起因として、ＴＣＰ管理テーブル４にコネクション情報を登録することにより、サーバ１９からクライアント１８への方向に関して、ＴＣＰコネクション単位で管理することができる。

【００８１】また、実施の形態２では、コネクション情報の登録からコネクション情報の有効化まで、コネクション情報が無効な期間が存在する。一方、実施の形態３では、一個のＳＹＮセグメント７２により、コネクション情報の登録とコネクション情報の有効化を同時に行うため、コネクション情報が無効な期間が存在しない。

【００８２】また、実施の形態２と実施の形態３により、ＴＣＰプロトコル通信を行う端末間の双方向のＴＣＰコネクションに関して、ラインカードＡ１Ａ及びラインカードＢ１Ｂがそれぞれ片方向のＴＣＰコネクションを管理するＴＣＰ管理テーブルを保有することができ、適切な通信パケット制御を行なうことができる。

【００８３】実施の形態４．本実施の形態では、実施の形態１で示したラインカード１の処理のうち、コネクション切断時の処理の詳細を説明する。

【００８４】ＴＣＰコネクションの切断を要求するためのＴＣＰセグメント２４には２種類ある。一つ目は、ＦＩＮビット３３がＯＮに設定されたＴＣＰセグメント２４であり、本明細書では、ＦＩＮセグメントと称する。二つ目は、ＲＳＴビット３５がＯＮに設定されたＴＣＰセグメント２４であり、本明細書では、ＲＳＴセグメントと称する。なお、ＦＩＮセグメントは、コネクション切断パケットに相当し、ＲＳＴセグメントはコネクション強制切断パケットに相当する。実施の形態４では、前者のＦＩＮセグメントによるＴＣＰコネクション切断を示す。また、実施の形態５では、後者のＲＳＴセグメントによるＴＣＰコネクション切断を示す。

【００８５】ＦＩＮセグメントによるＴＣＰコネクション切断では、ＴＣＰプロトコルで通信する端末間で、４個のセグメントを使用して行う。ＴＣＰプロトコル通信は双方向に独立して通信できるため、各方向が独立的にＴＣＰコネクションを切断しなければならない。そのため、クライアント１８とサーバ１９は両方から、ＦＩＮセグメントを発行して、ＴＣＰコネクション切断を要求する。

【００８６】ＴＣＰコネクション切断の動作を図１２を用いて説明する。なお、図１２において、記述のないＦＩＮビット３３、ＳＹＮビット３４、ＲＳＴビット３５、ＡＣＫビット３６は、ＯＦＦに設定されていることを意味する。

【００８７】第一に、クライアント１８からのＴＣＰコネクション切断の場合である。まず、第一フェーズとして、クライアント１８は、切断したいサーバ１９のポート番号を指定したＦＩＮセグメント１２１を、サーバ１９に対して送信する。次に、第二フェーズとして、サーバ１９は、クライアント１８からのＦＩＮセグメント１２１に対する応答であるＴＣＰセグメント１２２を、クライアント１８に対して送信する。その場合、フラグビット３２の内、ＡＣＫビット３６のみがＯＮに設定されている。また、確認応答番号３１には、クライアント１８が送信したＦＩＮセグメント１２１のシーケンス番号３０に１を加算した値が設定される。

【００８８】第二に、サーバ１９からのＴＣＰコネクション切断の場合である。まず、第一フェーズとして、サーバ１９は、切断したいクライアント１８のポート番号を指定したＦＩＮセグメント１２３を、クライアント１８に対して送信する。次に、第二フェーズとして、クライアント１８は、サーバ１９からのＦＩＮセグメント１２３に対する応答であるＴＣＰセグメント１２４を、サーバ１９に対して送信する。その場合、フラグビット３２の内、ＡＣＫビット３６のみがＯＮに設定されている。また、確認応答番号３１には、サーバ１９が送信したＦＩＮセグメント１２３のシーケンス番号３０に１を加算した値が設定される。

【００８９】但し、クライアント１８からのＴＣＰコネクション切断と、サーバ１９からのＴＣＰコネクション切断は、独立的に行われるため、必ずしも順番に行われるわけではない。

【００９０】ラインカード１では、ＴＣＰコネクションを切断するためのＦＩＮセグメントの受信を起因として、ＴＣＰ管理テーブル４から、コネクション情報を削除する。このコネクション情報の削除は、入力側ＴＣＰセグメント管理部２でのみ行う。

【００９１】図２の構成例では、クライアント１８からのＦＩＮセグメント１２１は、ラインカードＡ１Ａの入力側ＴＣＰセグメント管理部２で行う。ラインカードＡ１Ａでは、サーバ１９からのＦＩＮセグメント１２３に関しては、何も行わない。また、サーバ１９からのＦＩＮセグメント１２３は、ラインカードＢ１Ｂの入力側ＴＣＰセグメント管理部２で行う。ラインカードＢ１Ｂでは、クライアント１８からのＦＩＮセグメント１２１に関しては、何も行わない。

【００９２】図１３は、ＦＩＮセグメントによる、コネクション情報の削除処理のフローチャートである。但し、ＦＩＮセグメントによるＴＣＰコネクション切断と、ＲＳＴセグメントによるＴＣＰコネクション切断は同一処理であるため、図１３の各ステップの説明は、両方の場合について記述する。

25

【００９３】入力側フラグビット判定部５１は、ＴＣＰセグメント２４からフラグビット３２を抽出（ステップ１３１）し、ＦＩＮビット３３とＲＳＴビット３５の設定値から、ＴＣＰコネクション切断を要求するためのＴＣＰセグメント２４であるか否かを確認する（ステップ１３２）。ＦＩＮビット３３、または、ＲＳＴビット３５のいずれかがＯＮの場合は、ステップ１３３に進む。また、ＦＩＮビット３３とＲＳＴビット３５の両方がＯＦＦの場合は終了する。但し、入力側フラグビット判定部５１に渡されたＩＰパケットは、４種類（ＴＣＰコネクション確立、ＴＣＰコネクション切断、データ送信、送達確認）のいずれかに必ず該当するため、ここで示す終了とは、他の条件（ＴＣＰコネクション確立、データ送信、送達確認）の判定に進むことを意味する。実施の形態４では、ＦＩＮセグメントは、ＦＩＮビット３３がＯＮであるため、ステップ１３３に進む。

【００９４】入力側コネクション情報管理部５４は、ＩＰパケット２０内の、送信元ＩＰアドレス２６、送信元ポート番号２８、送信先ＩＰアドレス２７、送信先ポート番号２９を組合わせて、コネクション識別子４１を生成する（ステップ１３３）。次に、生成したコネクション識別子４１をキーとして、ＴＣＰ管理テーブル４を検索（ステップ１３４）し、コネクション情報が既に登録されているか否かを確認する（ステップ１３５）。

【００９５】コネクション情報が既にＴＣＰ管理テーブル４に登録されている場合は、現在のＴＣＰコネクションを切断するために、ステップ１３４で検出した情報をＴＣＰ管理テーブル４から削除する（ステップ１３６）。

【００９６】最後に、入力側コネクション情報管理部５４で処理されたＩＰパケット２０は、カード間送受信回路９を経由して、そのＩＰパケット２０を送出すべきラインカードに転送される（ステップ１３７）。

【００９７】このように、入力側ＴＣＰセグメント管理部２において、ＦＩＮセグメントの受信を起因として、ＴＣＰ管理テーブル４からコネクション情報を削除することにより、クライアント１８からサーバ１９へ、及び、サーバ１９からクライアント１８への両方向に対応することができる。

【００９８】実施の形態５．ＲＳＴセグメントによるＴＣＰコネクション切断では、ＴＣＰプロトコルで通信する端末間で、１個のセグメントを使用して行う。ＲＳＴセグメントは、クライアント１８、または、サーバ１９のいずれかが、強制的にＴＣＰコネクションを切断する場合に使用する。クライアント１８では、ＴＣＰプロトコルでの通信を中断する場合に、ＲＳＴセグメントを発行する。また、クライアント１８がサーバ１９の未使用ポート番号に対してコネクション要求した場合、サーバ１９は、その要求を拒否するためにＲＳＴセグメントを発行する。

26

【００９９】ラインカード１では、ＴＣＰコネクションを切断するためのＲＳＴセグメントの受信を起因として、ＴＣＰ管理テーブル４から、コネクション情報を削除する。このコネクション情報の削除は、入力側ＴＣＰセグメント管理部２と出力側ＴＣＰセグメント管理部３の両方で行う。クライアント１８からサーバ１９に対してＲＳＴセグメントが送信された場合には、ラインカードＡ１Ａの入力側ＴＣＰセグメント管理部２とラインカードＢ１Ｂの出力側ＴＣＰセグメント管理部３が処理を行い、サーバ１９からクライアント１８に対してＲＳＴセグメントが送信された場合には、ラインカードＢ１Ｂの入力側ＴＣＰセグメント管理部２とラインカードＡ１Ａの出力側ＴＣＰセグメント管理部３が処理を行う。ＲＳＴセグメントによるＴＣＰコネクション切断処理のフローは、図１３と同一であるため、説明は省略する。

【０１００】このように、ラインカードＡ１Ａ（又はラインカードＢ１Ｂ）では、入力側ＴＣＰセグメント管理部２において、ＲＳＴセグメントの受信を起因として、ＴＣＰ管理テーブル４からコネクション情報を削除することにより、クライアント１８（又はサーバ１９）からの強制的なＴＣＰコネクション切断に対応することができる。また、ラインカードＡ１Ａ（又はラインカードＢ１Ｂ）では、出力側ＴＣＰセグメント管理部３において、ＲＳＴセグメントの受信を起因として、ＴＣＰ管理テーブル４からコネクション情報を削除することにより、サーバ１９（又はクライアント１８）からの強制的なＴＣＰコネクション切断に対応することができる。

【０１０１】実施の形態６．本実施の形態では、実施の形態１で示したラインカード１の処理のうち、データ送信の際の処理の詳細を説明する。

【０１０２】図１４は、クライアント１８からサーバ１９へデータ転送した場合のシーケンスである。サーバ１９からクライアント１８へデータ転送した場合も同様に動作する。なお、図１４において、記述のないＦＩＮビット３３、ＳＹＮビット３４、ＲＳＴビット３５、ＡＣＫビット３６は、ＯＦＦに設定されていることを意味する。

【０１０３】ユーザデータを転送するＴＣＰセグメント２４は、ＦＩＮビット３３、ＳＹＮビット３４、ＲＳＴビット３５、ＡＣＫビット３６のすべてがＯＦＦに設定されている。本明細書では、このＴＣＰセグメント２４をＴＣＰデータセグメントと称する。なお、ＴＣＰデータセグメントは、データパケットに相当する。また、ユーザデータの送達確認用のＴＣＰセグメント２４は、ＡＣＫビット３６がＯＮに、かつ、ＦＩＮビット３３、ＳＹＮビット３４、ＲＳＴビット３５がＯＦＦに設定されている。本明細書では、このＴＣＰセグメント２４を送達確認セグメントと称する。なお、送達確認セグメントは、送達確認パケットに相当する。

【０１０４】ＴＣＰプロトコルでのデータ転送における

送達確認は、ＴＣＰデータセグメント毎に返答する場合と、複数個のＴＣＰデータセグメント毎に返答する場合がある。

【０１０５】第一に、前者のケースの動作を説明する。まず、第一フェーズとして、クライアント１８は、ＴＣＰデータセグメント１４１を、サーバ１９に対して送信する。図１４の例では、１００バイト長のデータを送信する。次に、第二フェーズとして、サーバ１９は、クライアント１８からのＴＣＰデータセグメント１４１に対する送達確認セグメント１４２を、クライアント１８に対して送信する。その場合、フラグビット３２の内、ＡＣＫビット３６のみＯＮに設定されている。また、確認応答番号３１には、クライアント１８からのＴＣＰデータセグメント１４１のシーケンス番号３０にデータサイズを加算した値が設定されている。図１４の例では、確認応答番号３１は、シーケンス番号３０の１００にデータサイズの１００を加算した２００の値が設定される。

【０１０６】第二に、後者のケースの動作を説明する。まず、第一フェーズとして、クライアント１８は、ＴＣＰデータセグメント１４３を、サーバ１９に対して送信する。図１４の例では、１００バイト長のデータを送信する。次に、第二フェーズとして、クライアント１８は、サーバからの送達確認を待たずに、ユーザデータを含むＴＣＰセグメント１４４を、サーバ１９に対して送信する。図１４の例では、１５０バイト長のデータを送信する。最後に、第三フェーズとして、サーバ１９は、クライアント１８からのＴＣＰデータセグメント１４２までの処理が完了したことを通知するため、送達確認セグメント１４５を、クライアント１８に対して送信する。その場合、フラグビット３２の内、ＡＣＫビット３６のみＯＮに設定されている。また、確認応答番号３１には、クライアント１８からのＴＣＰデータセグメント１４４のシーケンス番号３０にデータサイズを加算した値が設定されている。図１４の例では、確認応答番号３１は、シーケンス番号３０の３００にデータサイズの１５０を加算した４５０の値が設定される。

【０１０７】ラインカード１では、ＴＣＰデータセグメントの受信を起因として、入力側ＴＣＰセグメント管理部２で、ＴＣＰデータセグメントの正当性（連続したデータ列であること）を確認し、中継処理の要否を判断する。また、ＴＣＰデータセグメントが正当である場合は、ＴＣＰ管理テーブル４内の該当するコネクション情報のＳｅｑ番号４２を更新する。また、ラインカード１では、送達確認セグメントの受信を起因として、出力側ＴＣＰセグメント管理部３で、ＴＣＰ管理テーブル４内の該当するコネクション情報のＡｃｋ番号４３を更新する。

【０１０８】図１５は、ＴＣＰデータセグメントに対する処理のフローチャートである。

【０１０９】入力側フラグビット判定部５１は、ＴＣＰセグメント２４からフラグビット３２を抽出（ステップ１５１）し、ＴＣＰデータセグメントであるか否かを確認する（ステップ１５２）。ＴＣＰデータセグメントでない場合は終了する。但し、入力側フラグビット判定部５１に渡されたＩＰパケットは、４種類（ＴＣＰコネクション確立、ＴＣＰコネクション切断、データ送信、送達確認）のいずれかに必ず該当するため、ここで示す終了とは、他の条件（ＴＣＰコネクション確立、ＴＣＰコネクション切断、送達確認）の判定に進むことを意味する。実施の形態６では、ＴＣＰデータセグメントであるため、ステップ１５３に進む。

【０１１０】入力側コネクション情報管理部５４は、ＩＰパケット２０内の、送信元ＩＰアドレス２６、送信元ポート番号２８、送信先ＩＰアドレス２７、送信先ポート番号２９を組合わせて、コネクション識別子４１を生成する（ステップ１５３）。次に、生成したコネクション識別子４１をキーとして、ＴＣＰ管理テーブル４を検索（ステップ１５４）し、一致するコネクション識別子が登録されているか否かを確認する（ステップ１５５）。ＴＣＰ管理テーブル４に登録されていない場合は、ステップ１６３に進む。

【０１１１】コネクション識別子が登録されているケースとしては、ＴＣＰプロトコルでは、ＴＣＰデータセグメントの送信側（図１４の場合ではクライアント１８）が一定期間を超過しても送達確認を受けない場合がある。このとき、送信側はＴＣＰデータセグメントを再送する。しかし、送信側が送達確認を受けない要因には、ＩＰパケット２０がネットワークのどこかで廃棄された場合や、ＩＰパケット２０の転送遅延が送信側の許容時間を超えた場合など様々である。ステップ１５５～１５８は、受信側（図１４の場合ではサーバ１９）で受け取り済であるＴＣＰデータセグメントに関しては再送の必要がないため、フィルタ部５２は、それらのＴＣＰデータセグメントを検出して破棄することを目的としている。

【０１１２】ステップ１５５でＹｅｓの場合、フィルタ部５２は、まず、ＴＣＰデータセグメントのシーケンス番号３０と、ステップ１５４で検出したコネクション情報のＡｃｋ番号４３を比較（ステップ１５６）し、ＴＣＰデータセグメントのシーケンス番号３０が、コネクション情報のＡｃｋ番号４３より小さいか確認する（ステップ１５７）。ＴＣＰデータセグメントのシーケンス番号３０が、コネクション情報のＡｃｋ番号４３より小さい場合、そのＴＣＰデータセグメントは受信側で受け取り済であることを示すため、ＴＣＰデータを廃棄する（ステップ１５８）。

【０１１３】ＴＣＰプロトコルでは、連続したＴＣＰデータセグメントの一部が抜けた場合、受信側は抜けたＴＣＰデータセグメントからの再送を、送信側に対して要求する。そのため、連続したＴＣＰデータセグメントの

内、一つのＴＣＰデータセグメントが抜けた時点で、それに続くＴＣＰデータセグメントは意味を持たない。フィルタ部５２では、ＴＣＰデータセグメントの抜けを検出して、それ以降のＴＣＰデータセグメントを廃棄することを目的としている。

【０１１４】ステップ１５７でＮｏの場合、フィルタ部５２は、まず、ＴＣＰデータセグメントのシーケンス番号３０と、ステップ１５４で検出したコネクション情報のＳｅｑ番号４２を比較（ステップ１５９）し、ＴＣＰデータセグメントのシーケンス番号３０が、コネクション情報のＳｅｑ番号４２より大きいか確認する（ステップ１６０）。ＴＣＰデータセグメントのシーケンス番号３０が、コネクション情報のＳｅｑ番号４２より大きい場合、ＴＣＰデータセグメントの抜けが起きていることを示すため、ＴＣＰデータを廃棄する（ステップ１６１）。

【０１１５】ステップ１６０でＮｏの場合、Ｓｅｑ番号更新部５３は、ステップ１５４で検出したコネクション情報のＳｅｑ番号４２に、ＴＣＰデータセグメントのデータサイズを加算する（ステップ１６２）。ここで更新されたＳｅｑ番号４２の値は、次のＴＣＰデータセグメントのシーケンス番号３０の値（次中継シーケンス番号）である。

【０１１６】最後に、Ｓｅｑ番号更新部５３で処理されたＩＰパケット２０は、カード間送受信回路９を経由して、そのＩＰパケット２０を送出すべきラインカード１Ｂ～１Ｄに転送される（ステップ１６３）。

【０１１７】図１６は、送達確認セグメントに対する処理のフローチャートである。

【０１１８】出力側フラグビット判定部６１は、ＴＣＰセグメント２４からフラグビット３２を抽出（ステップ１７１）し、送達確認セグメントであるか否かを確認する（ステップ１７２）。送達確認セグメントでない場合は終了する。但し、出力側フラグビット判定部６１に渡されたＩＰパケットは、４種類（ＴＣＰコネクション確立、ＴＣＰコネクション切断、データ送信、送達確認）のいずれかに必ず該当するため、ここで示す終了とは、他の条件（ＴＣＰコネクション確立、ＴＣＰコネクション切断、データ送信）の判定に進むことを意味する。実施の形態６では、送達確認セグメントであるため、ステップ１７３に進む。

【０１１９】出力側コネクション情報管理部６３は、ＩＰパケット２０内の、送信先ＩＰアドレス２７、送信先ポート番号２９を組合わせて、送信元ＩＤ４５を生成する（ステップ１７３）。また、ＩＰパケット２０内の、送信元ＩＰアドレス２６、送信元ポート番号２８を組合わせて、送信先ＩＤ４６を生成する（ステップ１７４）。そして、ステップ１７３で生成した送信元ＩＤ４５と、ステップ１７４で生成した送信先ＩＤ４６を組合わせて、コネクション識別子４１を算出する（ステップ１７５）。出力側コネクション情報管理部６３では、入力側コネクション情報管理部５４と異なり、ＩＰパケット２０内の送信元／送信先を反転して、コネクション識別子４１を生成する。次に、生成したコネクション識別子４１をキーとして、ＴＣＰ管理テーブル４を検索（ステップ１７６）し、一致するコネクション識別子が既に登録されているか否かを確認する（ステップ１７７）。登録されている場合はステップ１７８に進み、登録されていない場合はステップ１７９に進む。

【０１２０】ステップ１７７でＹｅｓの場合は、Ａｃｋ番号更新部６２は、ステップ１７６で検出したコネクション情報のＡｃｋ番号４３に、送達確認セグメントの確認応答番号３１の値を設定する（ステップ１７８）。ここで更新されたＡｃｋ番号４３の値は、送信側が次に送信するＴＣＰセグメント２４のシーケンス番号３０の値であり、このシーケンス番号３０未満のＴＣＰデータセグメントは受信側で受け取り済みであることを示す。

【０１２１】最後に、Ａｃｋ番号更新部６２で処理されたＩＰパケット２０は、レイヤ２／３処理部８に渡される（ステップ１７９）。

【０１２２】図１７は、クライアント１８からサーバ１９に対して、２個の連続したデータＡ～データＢを送信する場合の例である。ここで、サーバ１９からの送達確認セグメント１８３が何らかの要因により転送遅延が大きくなり、クライアント１８がデータＡを含むＴＣＰデータセグメントを再送したと仮定する。なお、図１７におけるＴＣＰデータセグメントのデータサイズは、すべて５０バイトとする。

【０１２３】図１７を用いて、具体的な動作を説明する。ＩＰルータ１０は、データＡを含むＴＣＰデータセグメント１８１、及び、データＢを含むＴＣＰデータセグメント１８２に対するサーバ１９からの送達確認セグメント１８３を受信した時点で、ＴＣＰ管理テーブル４内の該当するコネクション情報のＡｃｋ番号４３を２００に設定する。その結果、ルータ１０は、次のＴＣＰセグメント２４のシーケンス番号３０は２００であると予測する。しかし、ルータ１０は、クライアント１８から再送されたデータＡを含むＴＣＰデータセグメント１８４を受信するため、ＴＣＰデータセグメント１８４のシーケンス番号３０とコネクション情報のＡｃｋ番号４３を比較した結果、データ重複と判定し、ルータ１０内で廃棄する。なお、既存の方式では、ＴＣＰデータセグメント１８４はルータ１０で廃棄されず、サーバ１９まで転送され、サーバ１９で廃棄するため、ルータ１０とサーバ１９の間のネットワークに無効なトラフィックが流れることになる。

【０１２４】このように、ルータ１０内のラインカード１において、出力側ＴＣＰセグメント管理部３でコネクション情報のＡｃｋ番号４３を管理して、ＴＣＰプロトコル通信における受信側が受け取り済みのＴＣＰセグメ

ント２４を把握することにより、従来は受信端末で廃棄していたデータをルータ１０内のラインカード１（入力側ＴＣＰセグメント管理部２）で早期検出して廃棄することにより、データ重複による無効なトラフィックを削減することができる。

【０１２５】図１８は、クライアント１８からサーバ１９に対して、４個の連続したデータＡ～データＤを送信する場合の例である。ここで、クライアント１８とルータ１０の間のネットワークにおいて、データＢを含むＴＣＰセグメント１８２が廃棄されたと仮定する。なお、図１８におけるＴＣＰデータセグメントは、すべて５０バイトとする。

【０１２６】図１８を用いて、具体的な動作を説明する。まず、ルータ１０は、クライアント１８からのデータＡを含むＴＣＰデータセグメント１９１を受信すると、ＴＣＰ管理テーブル４内の該当するコネクション情報のＳｅｑ番号４２を１５０に設定し、次のＴＣＰセグメント２４のシーケンス番号３０は１５０であると予測する。しかし、ルータ１０は、クライアント１８から次にデータＣを含むＴＣＰデータセグメント１９３を受信するため、ＴＣＰデータセグメント１９３のシーケンス番号３０とコネクション情報のＳｅｑ番号４２を比較した結果、データ抜けと判定し、ルータ１０内で廃棄する。なお、既存の方式では、サーバ１９までＴＣＰデータセグメント１９３～１９４は転送され、サーバ１９で廃棄するため、ルータ１０とサーバ１９の間のネットワークに無効なトラフィックが流れることになる。また、後続するデータＤを含むＴＣＰデータセグメント１９４に対しても、同様に廃棄する。

【０１２７】サーバ１９は、クライアント１８からのデータＡを含むＴＣＰデータセグメント１９１は正常に受信したため、送達確認セグメント１９５をクライアント１８に送信する。クライアント１８では、送達確認セグメント１９５を受信した後、ＴＣＰデータセグメント１９２～１９４に対する送達確認がないため、一定時間を経過すると、データＢ～データＤを含むＴＣＰデータセグメント１９６～１９８を再送する。

【０１２８】サーバ１９は、クライアント１８からのデータＢ～データＤを含むＴＣＰデータセグメント１９６～１９８を正常に受信したため、送達確認セグメント１９９をクライアント１８に送信する。

【０１２９】このように、ルータ１０内のラインカード１において、入力側ＴＣＰセグメント管理部２でコネクション情報のＳｅｑ番号４２を管理して、ラインカード１が次に受信するＴＣＰセグメント２４を予測することにより、従来は受信端末で廃棄していたデータをルータ１０内のラインカード１（入力側ＴＣＰセグメント管理部２）で早期検出して廃棄することにより、データ抜けによる無効なトラフィックを削減することができる。

【０１３０】また、データ重複やデータ抜けによる無効なトラフィックを削減することにより、ネットワークにおける輻輳が減り、ネットワーク全体の利用効率を向上させることができる。

【０１３１】なお、以上の実施の形態１～６では、中継処理装置の例としてラインカードを用いた場合について説明したが、これに限るものではなく、実施の形態１～６に示した処理を実現できるものであれば、ラインカード以外のものでもよい。

【０１３２】また、以上の実施の形態１～６では、ＴＣＰプロトコルを利用するＩＰパケットを前提として説明したが、これに限るものではなく、他の通信プロトコルを利用するデータにも適用することができる。

【０１３３】また、以上の実施の形態１～６では、本発明に係る中継処理装置について説明したが、実施の形態１～６に示した処理手順と同様の手順により、本発明に係る中継処理方法も実現することができる。

【０１３４】ここで、実施の形態１～６で示したラインカードの特徴を以下にて再言する。

【０１３５】実施の形態１～６のラインカードは、ＬＡＮまたはＷＡＮに接続されるラインカードにおいて、単一方向のＴＣＰコネクション毎に、コネクション情報を管理するＴＣＰ管理テーブルと、ＬＡＮまたはＷＡＮから受信したＩＰパケットのトランスポート層のプロトコル種別を判別して、前記トランスポート層にＴＣＰプロトコルを使用する前記ＩＰパケットを入力側ＴＣＰセグメント管理部に渡し、それ以外の前記ＩＰパケットをそのまま中継する入力フレーム種別判定部と、前記入力フレーム種別判定部から渡された前記トランスポート層にＴＣＰプロトコルを使用する前記ＩＰパケットを受けて、前記ＴＣＰ管理テーブルの制御、及び、ＴＣＰセグメントの正当性の確認を行う入力側ＴＣＰセグメント管理部と、他のラインカードから中継されたＩＰパケットのトランスポート層のプロトコル種別を判別して、前記トランスポート層にＴＣＰプロトコルを使用する前記ＩＰパケットを出力側ＴＣＰセグメント管理部に渡し、それ以外の前記ＩＰパケットをそのまま中継する出力フレーム種別判定部と、前記出力フレーム種別判定部から渡された前記トランスポート層にＴＣＰプロトコルを使用する前記ＩＰパケットを受けて、前記ＴＣＰ管理テーブルの制御を行う出力側ＴＣＰセグメント管理部と、を備えたことを特徴とする。

【０１３６】実施の形態１～６のラインカードは、単一方向のＴＣＰコネクション毎に、送信元のＴＣＰソケットと送信先のＴＣＰソケットを組合せたコネクション識別子と、前記ラインカードが次に受信するデータ送信用ＴＣＰセグメントのシーケンス番号を記録するＳｅｑ番号と、前記ラインカードが受信した最新の送達確認用ＴＣＰセグメントの確認応答番号を記録するＡｃｋ番号と、前記コネクション識別子と前記Ｓｅｑ番号と前記Ａｃｋ番号を組合せた情報であるコネクション情報の有効

33

性を示す確立フラグから構成されるＴＣＰ管理テーブルと、を有することを特徴とする。

【０１３７】実施の形態１～６のラインカード内の入力側ＴＣＰセグメント管理部は、トランスポート層にＴＣＰプロトコル層を使用するＩＰパケットのフラグビットにより、前記ＩＰパケット内のＴＣＰセグメントの種別を判定する入力側フラグビット判定部と、前記入力側フラグビット判定部で、ＴＣＰコネクション確立用またはＴＣＰコネクション切断用と判定された前記ＴＣＰセグメントの内容に基づき、前記ＴＣＰ管理テーブルに前記コネクション情報を登録または削除する入力側コネクション情報管理部と、前記入力側フラグビット判定部で、データ送信用と判定された前記ＴＣＰセグメントに関して、前記ＴＣＰ管理テーブルを参照して、前記ＴＣＰセグメントの正当性を確認するフィルタ部と、前記入力側フラグビット判定部で、データ送信用と判定された前記ＴＣＰセグメントの内容に基づき、前記ＴＣＰ管理テーブル内の該当する前記コネクション情報のＳｅｑ番号を更新するＳｅｑ番号更新部と、定期的に前記ＴＣＰ管理テーブルの前記確立フラグを監視し、前記コネクション情報の有効性を確認するコネクション確認部と、を有することを特徴とする。

【０１３８】実施の形態１～６のラインカード内の出力側ＴＣＰセグメント管理部は、トランスポート層にＴＣＰプロトコル層を使用するＩＰパケットのフラグビットにより、前記ＩＰパケット内のＴＣＰセグメントの種別を判定する出力側フラグビット判定部と、前記出力側フラグビット判定部で、ＴＣＰコネクション確立用またはＴＣＰコネクション切断用と判定された前記ＴＣＰセグメントの内容に基づき、前記ＴＣＰ管理テーブルに前記コネクション情報を登録または削除する出力側コネクション情報管理部と、前記出力側フラグビット判定部で、送達確認用と判定された前記ＴＣＰセグメントの内容に基づき、前記ＴＣＰ管理テーブル内の該当する前記コネクション情報のＡｃｋ番号を更新するＡｃｋ番号更新部と、を有することを特徴とする。

【０１３９】実施の形態２のラインカードは、ＴＣＰコネクション確立シーケンスの第一フェーズにおける、クライアントがＴＣＰコネクションを確立するためのＴＣＰセグメントであるＳＹＮセグメントの受信を起因とし、前記入力側ＴＣＰセグメント管理部で、前記ＴＣＰ管理テーブルへの前記コネクション情報の登録を行い、前記出力側ＴＣＰセグメント管理部で、前記コネクション情報の有効化を行うことを特徴とする。

【０１４０】実施の形態２のラインカードは、定期的に前記ＴＣＰ管理テーブルの前記確立フラグを監視し、ＴＣＰプロトコル通信を行う端末間で、双方向のＴＣＰコネクションの確立していない前記コネクション情報を削除することを特徴とする。

【０１４１】実施の形態３のラインカードは、ＴＣＰコネクション確立シーケンスの第二フェーズにおける、サーバがＴＣＰコネクションを確立するためのＴＣＰセグメントであるＳＹＮセグメントの受信を起因とし、前記入力側ＴＣＰセグメント管理部で、前記ＴＣＰ管理テーブルへの前記コネクション情報の登録、及び、前記コネクション情報の有効化を同時に行うことを特徴とする。

34

【０１４２】実施の形態４、５のラインカードは、クライアントがＴＣＰコネクションを切断するためのＴＣＰセグメントであるＦＩＮセグメント、または、クライアントがＴＣＰコネクションを強制的に切断するためのＴＣＰセグメントであるＲＳＴセグメントの受信を起因とし、前記入力側ＴＣＰセグメント管理部で、前記ＦＩＮセグメントまたは前記ＲＳＴセグメントのコネクション識別子を算出し、前記コネクション識別子をキーとして、前記ＴＣＰ管理テーブル内から該当する前記コネクション情報を特定し、前記ＴＣＰ管理テーブルから前記コネクション情報を削除することを特徴とする。

【０１４３】実施の形態５のラインカードは、サーバがＴＣＰコネクションを強制的に切断するためのＴＣＰセグメントであるＲＳＴセグメントの受信を起因とし、前記出力側ＴＣＰセグメント管理部で、前記ＲＳＴセグメントのコネクション識別子を算出し、前記コネクション識別子をキーとして、前記ＴＣＰ管理テーブル内から該当する前記コネクション情報を特定し、前記ＴＣＰ管理テーブルから前記コネクション情報を削除することを特徴とする。

【０１４４】実施の形態６のラインカードは、ユーザデータを含むＴＣＰセグメントであるＴＣＰデータセグメントの受信を起因とし、前記入力側ＴＣＰセグメント管理部で、前記ＴＣＰデータセグメントのコネクション識別子を算出し、前記コネクション識別子をキーとして、前記ＴＣＰ管理テーブル内から該当する前記コネクション情報を特定し、前記コネクション情報のＳｅｑ番号を、前記ＴＣＰデータセグメントのデータサイズを加算した値に更新することを特徴とする請求項１に記載の通信パケット制御方式。

【０１４５】実施の形態６のラインカードは、前記ＴＣＰデータセグメントの送達確認用のＴＣＰセグメントである送達確認セグメントの受信を起因とし、前記出力側ＴＣＰセグメント管理部で、前記送達確認セグメントのコネクション識別子を算出し、前記コネクション識別子をキーとして、前記ＴＣＰ管理テーブル内から該当する前記コネクション情報を特定し、前記コネクション情報のＡｃｋ番号を、前記送達確認セグメントの確認応答番号の値に更新することを特徴とする。

【０１４６】実施の形態６のラインカードは、ユーザデータを含むＴＣＰセグメントであるＴＣＰデータセグメントに関して、前記入力側ＴＣＰセグメント管理部で、前記ＴＣＰデータセグメントのコネクション識別子を算出し、前記コネクション識別子をキーとして、前記ＴＣ

Ｐ管理テーブル内から該当する前記コネクション情報を特定し、前記コネクション情報のＡｃｋ番号と、前記ＴＣＰデータセグメントのシーケンス番号を比較して、受信側で受け取り済みのＴＣＰデータセグメントを検出し、前記受信側で受け取り済みのＴＣＰデータセグメントを廃棄することを特徴とする。

【０１４７】実施の形態６のラインカードは、ユーザデータを含むＴＣＰセグメントであるＴＣＰデータセグメントに関して、前記入力側ＴＣＰセグメント管理部で、前記ＴＣＰデータセグメントのコネクション識別子を算出し、前記コネクション識別子をキーとして、前記ＴＣＰ管理テーブル内から該当する前記コネクション情報を特定し、前記コネクション情報のＳｅｑ番号と、前記ＴＣＰデータセグメントのシーケンス番号を比較して、連続した前記ＴＣＰデータセグメントの一部が抜けたことを検出し、抜けた前記ＴＣＰデータセグメントに続く前記ＴＣＰデータセグメントを廃棄することを特徴とする。

【０１４８】

【発明の効果】本発明によれば、データパケットが受信される度に、中継要否判断部がデータパケットの送信シーケンス番号と通信管理テーブルに記憶された判断基準シーケンス番号とを比較して中継処理の要否判断を行うため、従来はパケット受信側で破棄していた無効なデータパケットを早期に検出することができ、これにより無効なデータパケットの中継を削減することが可能になり、ネットワークにおける輻輳を減らし、ネットワーク全体の利用効率を向上させることができる。

【０１４９】また、本発明によれば、中継要否判断部は次中継シーケンス番号を算出し、通信管理テーブルは次中継シーケンス番号のうち最新の次中継シーケンス番号を記憶し、中継要否判断部はデータパケットの送信シーケンス番号と通信管理テーブルに記憶された次中継シーケンス番号とを比較して中継処理の要否判断を行うため、従来はパケット受信側で破棄していたデータ抜けによる無効なデータパケットを早期に検出することができ、これにより無効なデータパケットの中継を削減することが可能となり、ネットワークにおける輻輳を減らし、ネットワーク全体の利用効率を向上させることができる。

【０１５０】また、本発明によれば、通信管理テーブルは確認シーケンス番号のうち最新の確認シーケンス番号を記憶し、中継要否判断部はデータパケットの送信シーケンス番号と通信管理テーブルに記憶された確認シーケンス番号とを比較して中継処理の要否判断を行うため、従来はパケット受信側で破棄していたデータ重複による無効なデータパケットを早期に検出することができ、これにより無効なデータパケットの中継を削減することが可能となり、ネットワークにおける輻輳を減らし、ネットワーク全体の利用効率を向上させることができる。

【０１５１】また、本発明によれば、通信管理テーブルは次中継シーケンス番号と確認シーケンス番号とをコネクション識別子情報に対応づけて記憶し、中継要否判断部は、コネクション識別子情報に基づき対応する次中継シーケンス番号と確認シーケンス番号とを特定し、特定した次中継シーケンス番号及び確認シーケンス番号とデータパケットの送信シーケンス番号とを比較するため、双方向の通信コネクションのうち単一方向の通信コネクション単位でデータ抜けやデータ重複を検出することができ、ネットワークにおける輻輳を減らし、ネットワーク全体の利用効率を向上させることができる。

【０１５２】また、本発明によれば、通信管理テーブルはコネクション設定パケットの受信時にコネクション識別子情報を記憶し、コネクション管理部は応答コネクション設定パケットの受信時に通信コネクションの確立の判断を行うため、以降のデータパケットの中継処理要否判断において双方向の通信コネクションのうち単一方向の通信コネクション単位でデータ抜けやデータ重複を検出することができ、ネットワークにおける輻輳を減らし、ネットワーク全体の利用効率を向上させることができる。

【０１５３】また、本発明によれば、コネクション確認部が一定周期ごとに通信管理テーブルを検査して無効なコネクション識別子情報を削除するため、通信管理テーブルのリソースの浪費を防止することができる。

【０１５４】また、本発明によれば、コネクション管理部は応答コネクション設定パケットの受信時にコネクション識別子情報の登録と通信コネクションの確立の判断を行うため、コネクション識別子情報が無効な期間が存在せず、コネクション確立有無の確認処理を不要とすることができる。

【０１５５】本発明によれば、コネクション管理部は特定ネットワーク通信装置よりコネクション切断パケットを受信した場合に、対応するコネクション識別子情報を通信管理テーブルより削除するため、特定ネットワーク通信装置からのコネクション切断要求に対応することができる。

【０１５６】本発明によれば、コネクション管理部は特定ネットワーク通信装置よりコネクション強制切断パケットを受信した場合に、対応するコネクション識別子情報を通信管理テーブルより削除するため、特定ネットワーク通信装置からのコネクション強制切断要求に対応することができる。

【０１５７】本発明によれば、コネクション管理部は他ネットワーク通信装置よりコネクション強制切断パケットを受信した場合に、対応するコネクション識別子情報を通信管理テーブルより削除するため、他ネットワーク通信装置からのコネクション強制切断要求に対応することができる。

【図面の簡単な説明】

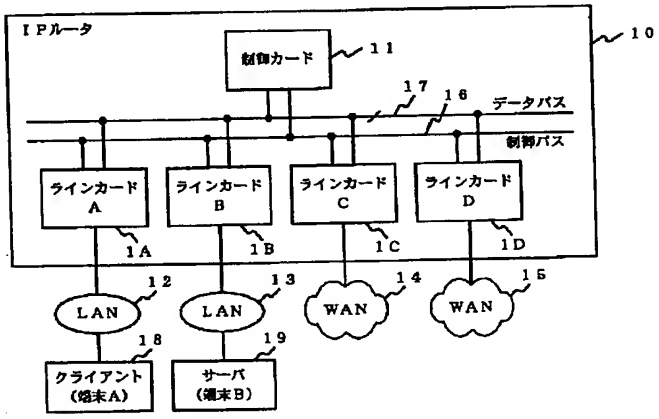
37

【図１】　実施の形態１～６のネットワーク構成例を示す図。
【図２】　ラインカードの内部構成例を示す図。
【図３】　ＩＰパケットのデータ構成例を示す図。
【図４】　ＩＰパケット内のフラグビットのデータ構成例を示す図。
【図５】　ＴＣＰ管理テーブルの構成例を示す図。
【図６】　ラインカード内の入力側ＴＣＰセグメント管理部の内部構成例を示す図。
【図７】　ラインカード内の出力側ＴＣＰセグメント管理部の内部構成例を示す図。
【図８】　コネクション確立時の通信シーケンスを示す図。
【図９】　コネクション確立時のラインカード内の入力側ＴＣＰセグメント管理部の処理を示すフローチャート図。
【図１０】　コネクション確立時のラインカード内の出力側ＴＣＰセグメント管理部の処理を示すフローチャート図。
【図１１】　ラインカード内のコネクション確認部の処理を示すフローチャート図。
【図１２】　コネクション切断時の通信シーケンスを示す図。
【図１３】　コネクション切断時のラインカード内の入

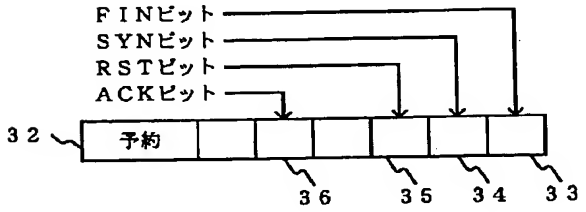
38

力側ＴＣＰセグメント管理部の処理を示すフローチャート図。
【図１４】　データ送信時の通信シーケンスを示す図。
【図１５】　データ送信時のラインカード内の入力側ＴＣＰセグメント管理部の処理を示すフローチャート図。
【図１６】　データ送信時のラインカード内の出力側ＴＣＰセグメント管理部の処理を示すフローチャート図。
【図１７】　データ送信時の通信シーケンスを示す図。
【図１８】　データ送信時の通信シーケンスを示す図。
【図１９】　従来の技術を示す図。
【符号の説明】
１　ラインカード、２　入力側ＴＣＰセグメント管理部、３　出力側ＴＣＰセグメント管理部、４　ＴＣＰ管理テーブル、５　入力フレーム種別判定部、６出力フレーム種別判定部、７　ネットワーク送受信回路、８　レイヤ２／３処理部、９　カード間送受信回路、１０　ＩＰルータ、１１　制御カード、１２　ＬＡＮ、１３　ＬＡＮ、１４　ＷＡＮ、１５　ＷＡＮ、１６　制御バス、１７　データバス、１８　クライアント、１９　サーバ、５１　入力側フラグビット判定部、５２　フィルタ部、５３　Ｓｅｑ番号更新部、５４　入力側コネクション情報管理部、５５　コネクション確認部、６１　出力側フラグビット判定部、６２Ａｃｋ番号更新部、６３　出力側コネクション情報管理部。

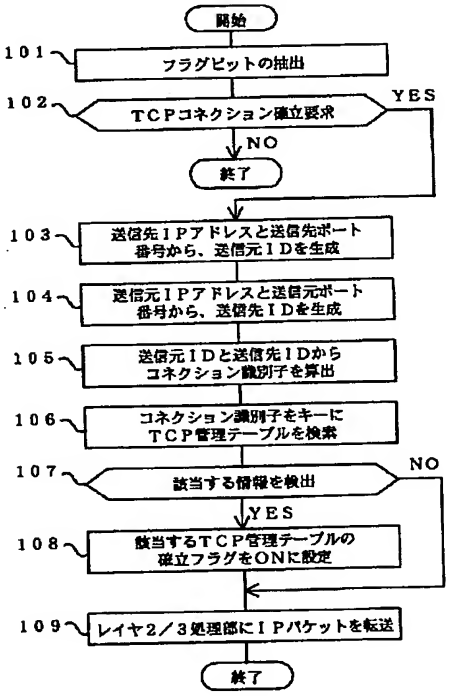
【図１】



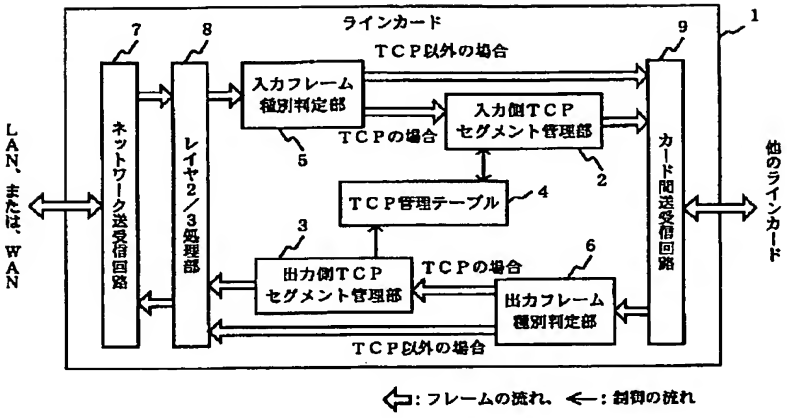
【図４】



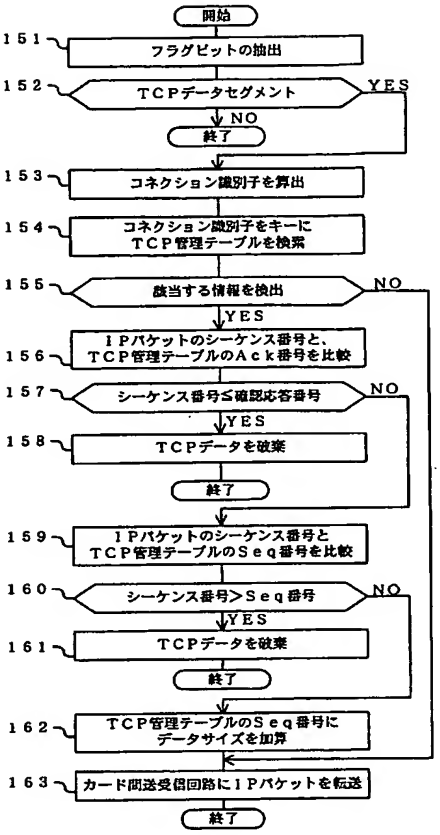
【図１０】



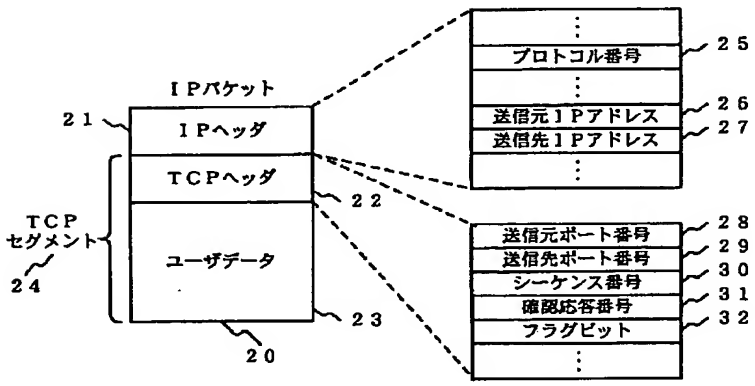
【図２】



【図１５】



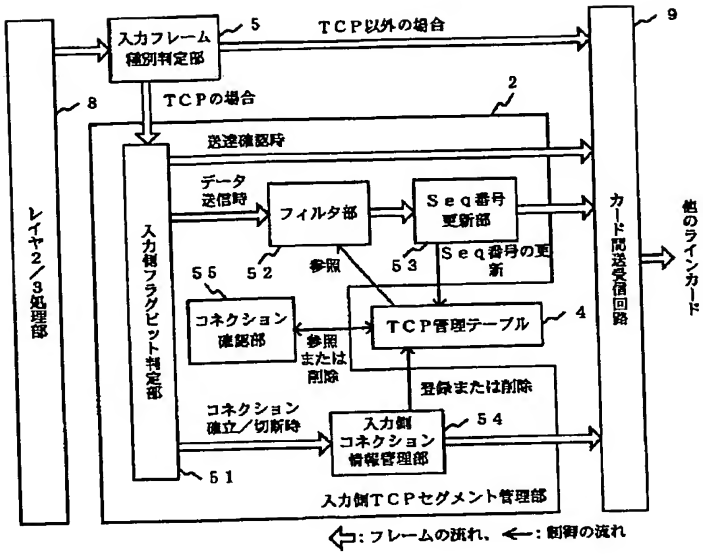
【図３】



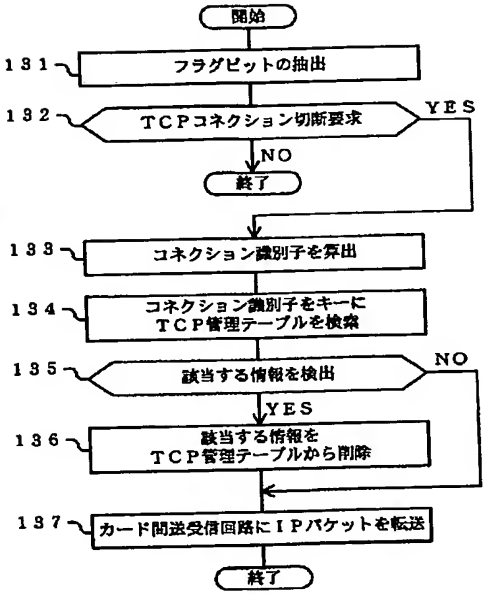
【図５】

45	41 コネクション識別子		42	43	44
	送信元ＩＤ	46 送信先ＩＤ	Ｓｅｑ番号	Ａｃｋ番号	確立フラグ
	端末A ポートX	端末B ポートY	１２	１０	ＯＮ
	端末B ポートW	端末A ポートZ	１３８	１３８	ＯＦＦ
4	⋮	⋮	⋮	⋮	⋮

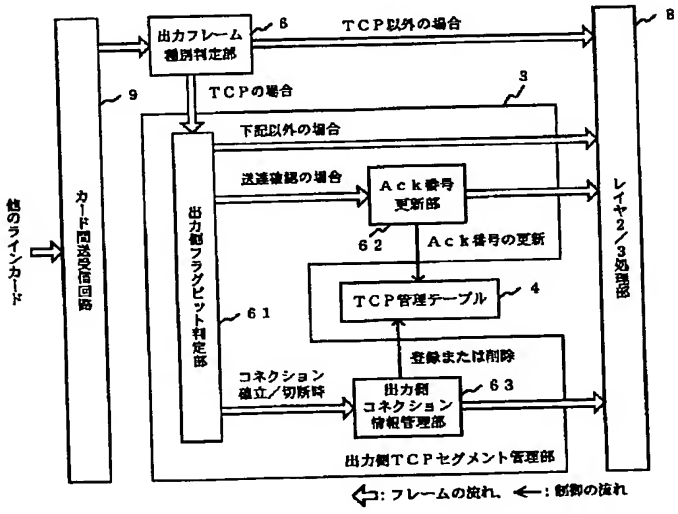
【図６】


入力フレーム種別判定部
5
TCP以外の場合
9
8
TCPの場合
2
送達確認時
データ送信時
フィルタ部
Seq番号更新部
レイヤ2／3処理部
入力側フラグビット判定部
カード間送受信回路
他のラインカード
55
52
参照
53
Seq番号の更新
コネクション確認部
TCP管理テーブル
4
参照または削除
登録または削除
コネクション確立／切断時
入力側コネクション情報管理部
54
51
入力側TCPセグメント管理部
⇦：フレームの流れ、←：制御の流れ

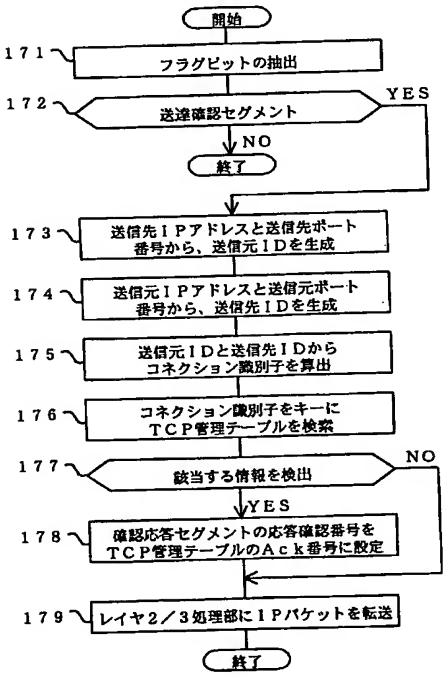
【図１３】


開始
131
フラグビットの抽出
132
TCPコネクション切断要求
YES
NO
終了
133
コネクション識別子を算出
134
コネクション識別子をキーにTCP管理テーブルを検索
135
該当する情報を検出
NO
YES
136
該当する情報をTCP管理テーブルから削除
137
カード間送受信回路にIPパケットを転送
終了

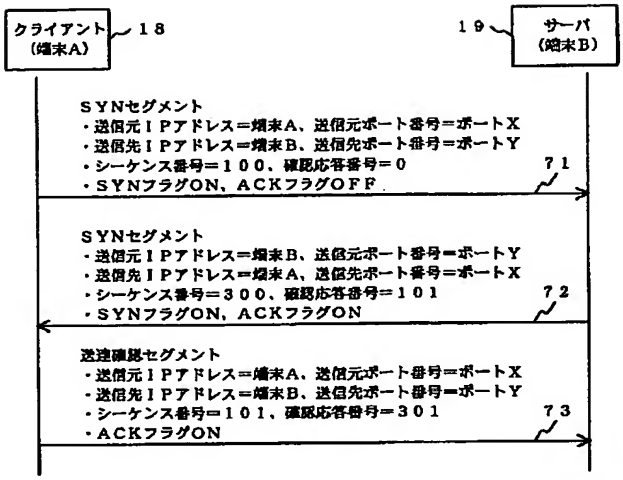
【図７】


出力フレーム種別判定部
8
TCP以外の場合
8
9
TCPの場合
3
下記以外の場合
送達確認の場合
Ack番号更新部
レイヤ2／3処理部
他のラインカード
カード間送受信回路
出力側フラグビット判定部
62
Ack番号の更新
TCP管理テーブル
4
61
登録または削除
コネクション確立／切断時
出力側コネクション情報管理部
63
出力側TCPセグメント管理部
⇦：フレームの流れ、←：制御の流れ

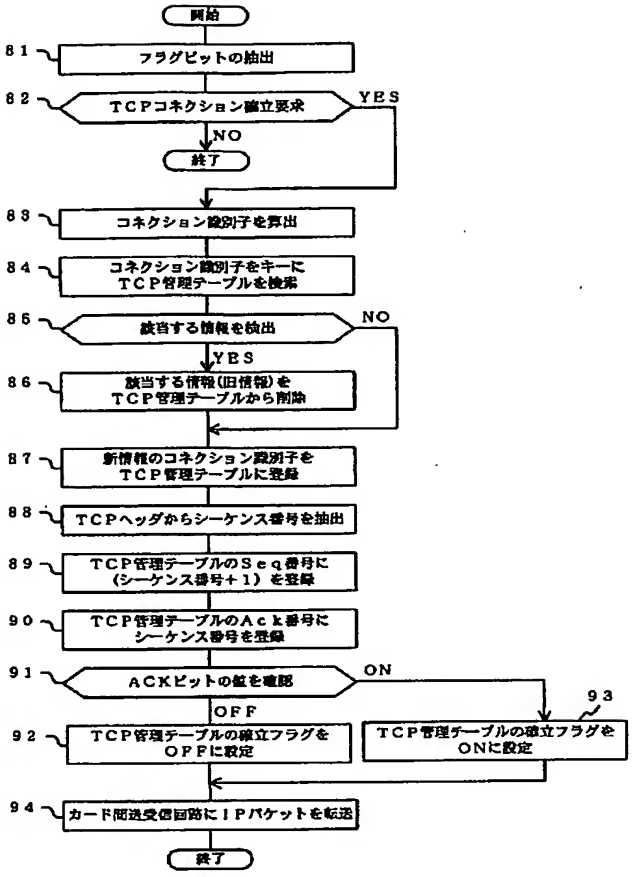
【図１６】


開始
171
フラグビットの抽出
172
送達確認セグメント
YES
NO
終了
173
送信先IPアドレスと送信先ポート番号から、送信元IDを生成
174
送信元IPアドレスと送信元ポート番号から、送信先IDを生成
175
送信元IDと送信先IDからコネクション識別子を算出
176
コネクション識別子をキーにTCP管理テーブルを検索
177
該当する情報を検出
NO
YES
178
確認応答セグメントの応答確認番号をTCP管理テーブルのAck番号に設定
179
レイヤ2／3処理部にIPパケットを転送
終了

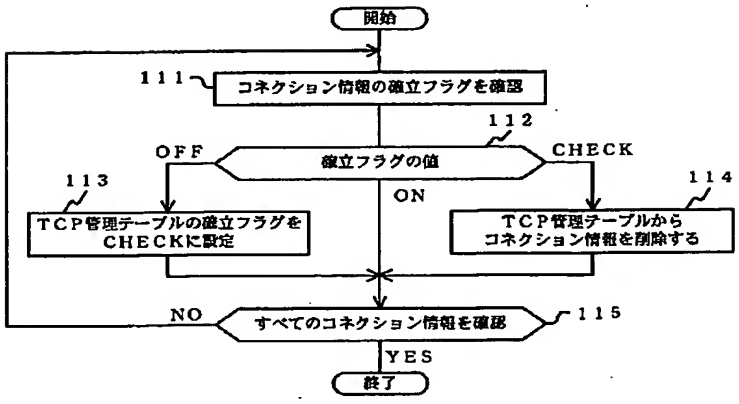
【図８】


クライアント
（端末A）
18
19
サーバ
（端末B）
SYNセグメント
・送信元ＩＰアドレス＝端末A、送信元ポート番号＝ポートX
・送信先ＩＰアドレス＝端末B、送信先ポート番号＝ポートY
・シーケンス番号＝１００、確認応答番号＝０
・SYNフラグON、ACKフラグOFF
71
SYNセグメント
・送信元ＩＰアドレス＝端末B、送信元ポート番号＝ポートY
・送信先ＩＰアドレス＝端末A、送信先ポート番号＝ポートX
・シーケンス番号＝３００、確認応答番号＝１０１
・SYNフラグON、ACKフラグON
72
送達確認セグメント
・送信元ＩＰアドレス＝端末A、送信元ポート番号＝ポートX
・送信先ＩＰアドレス＝端末B、送信先ポート番号＝ポートY
・シーケンス番号＝１０１、確認応答番号＝３０１
・ACKフラグON
73

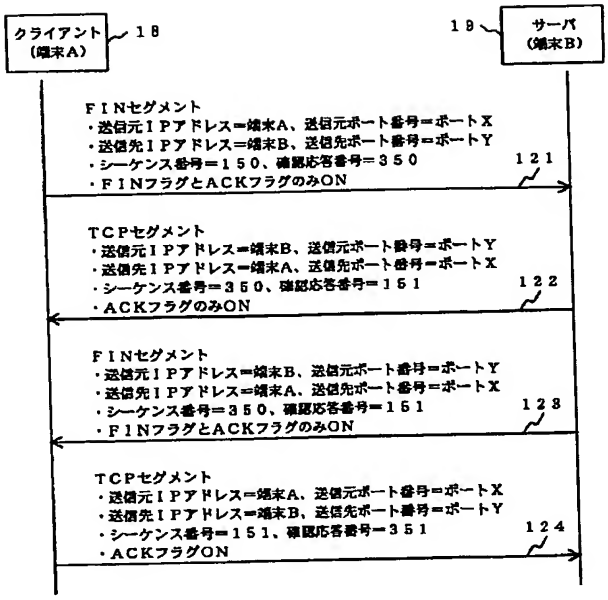
【図９】


開始
81
フラグビットの抽出
82
TCPコネクション確立要求
YES
NO
終了
83
コネクション識別子を算出
84
コネクション識別子をキーに
TCP管理テーブルを検索
85
該当する情報を検出
NO
YES
86
該当する情報（旧情報）を
TCP管理テーブルから削除
87
新情報のコネクション識別子を
TCP管理テーブルに登録
88
TCPヘッダからシーケンス番号を抽出
89
TCP管理テーブルのＳｅｑ番号に
（シーケンス番号＋１）を登録
90
TCP管理テーブルのＡｃｋ番号に
シーケンス番号を登録
91
ACKビットの値を確認
ON
OFF
93
92
TCP管理テーブルの確立フラグを
OFFに設定
TCP管理テーブルの確立フラグを
ONに設定
94
カード間送受信回路にＩＰパケットを転送
終了

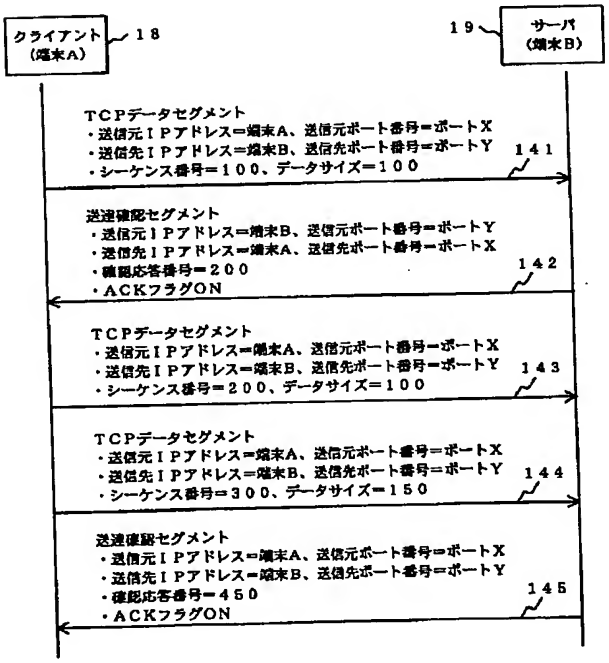
【図１１】


開始
111
コネクション情報の確立フラグを確認
112
OFF
確立フラグの値
CHECK
113
ON
114
TCP管理テーブルの確立フラグを
CHECKに設定
TCP管理テーブルから
コネクション情報を削除する
NO
すべてのコネクション情報を確認
115
YES
終了

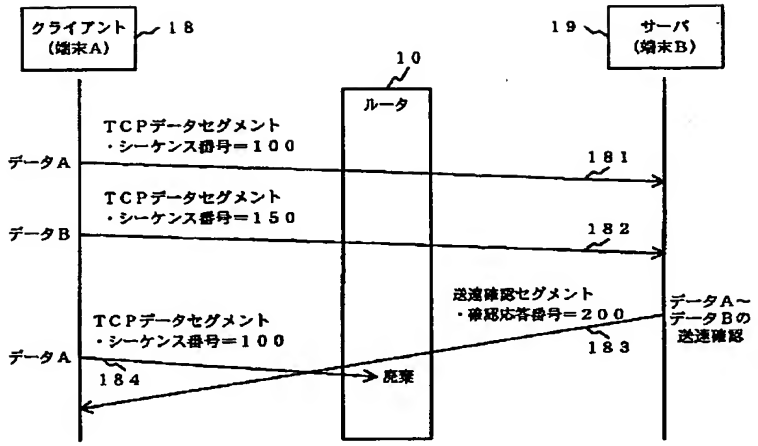
【図１２】


クライアント
（端末A）
18
19
サーバ
（端末B）
ＦＩＮセグメント
・送信元ＩＰアドレス＝端末A、送信元ポート番号＝ポートＸ
・送信先ＩＰアドレス＝端末B、送信先ポート番号＝ポートＹ
・シーケンス番号＝１５０、確認応答番号＝３５０
・ＦＩＮフラグとＡＣＫフラグのみＯＮ
121
ＴＣＰセグメント
・送信元ＩＰアドレス＝端末B、送信元ポート番号＝ポートＹ
・送信先ＩＰアドレス＝端末A、送信先ポート番号＝ポートＸ
・シーケンス番号＝３５０、確認応答番号＝１５１
・ＡＣＫフラグのみＯＮ
122
ＦＩＮセグメント
・送信元ＩＰアドレス＝端末B、送信元ポート番号＝ポートＹ
・送信先ＩＰアドレス＝端末A、送信先ポート番号＝ポートＸ
・シーケンス番号＝３５０、確認応答番号＝１５１
・ＦＩＮフラグとＡＣＫフラグのみＯＮ
123
ＴＣＰセグメント
・送信元ＩＰアドレス＝端末A、送信元ポート番号＝ポートＸ
・送信先ＩＰアドレス＝端末B、送信先ポート番号＝ポートＹ
・シーケンス番号＝１５１、確認応答番号＝３５１
・ＡＣＫフラグＯＮ
124

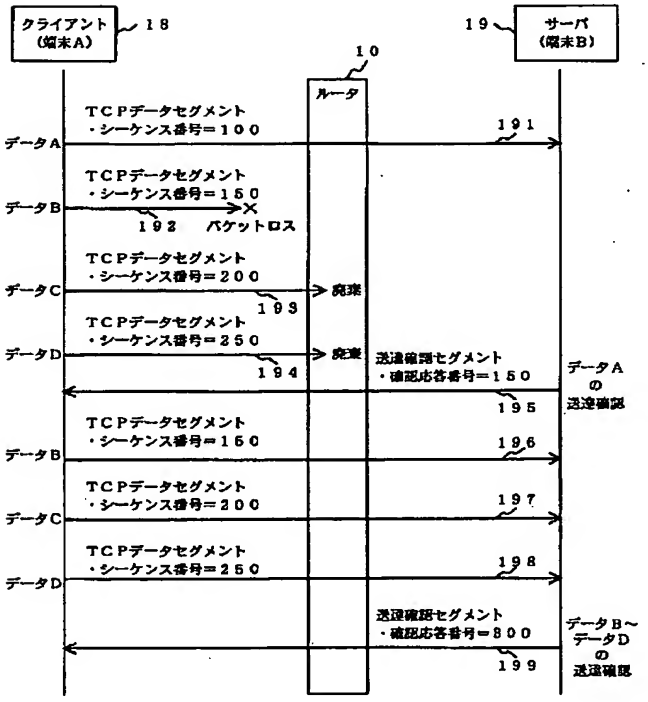
【図１４】


クライアント
（端末A）
18
19
サーバ
（端末B）
ＴＣＰデータセグメント
・送信元ＩＰアドレス＝端末A、送信元ポート番号＝ポートＸ
・送信先ＩＰアドレス＝端末B、送信先ポート番号＝ポートＹ
・シーケンス番号＝１００、データサイズ＝１００
141
送達確認セグメント
・送信元ＩＰアドレス＝端末B、送信元ポート番号＝ポートＹ
・送信先ＩＰアドレス＝端末A、送信先ポート番号＝ポートＸ
・確認応答番号＝２００
・ＡＣＫフラグＯＮ
142
ＴＣＰデータセグメント
・送信元ＩＰアドレス＝端末A、送信元ポート番号＝ポートＸ
・送信先ＩＰアドレス＝端末B、送信先ポート番号＝ポートＹ
・シーケンス番号＝２００、データサイズ＝１００
143
ＴＣＰデータセグメント
・送信元ＩＰアドレス＝端末A、送信元ポート番号＝ポートＸ
・送信先ＩＰアドレス＝端末B、送信先ポート番号＝ポートＹ
・シーケンス番号＝３００、データサイズ＝１５０
144
送達確認セグメント
・送信元ＩＰアドレス＝端末A、送信元ポート番号＝ポートＸ
・送信先ＩＰアドレス＝端末B、送信先ポート番号＝ポートＹ
・確認応答番号＝４５０
・ＡＣＫフラグＯＮ
145

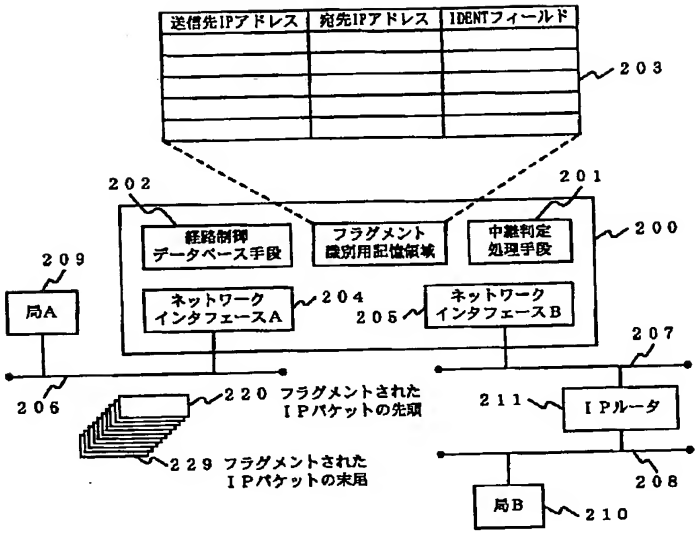
【図１７】


クライアント
(端末A)
18
19
サーバ
(端末B)
10
ルータ
TCPデータセグメント
・シーケンス番号＝１００
データA
181
TCPデータセグメント
・シーケンス番号＝１５０
データB
182
送達確認セグメント
・確認応答番号＝２００
データA～
データBの
送達確認
183
TCPデータセグメント
・シーケンス番号＝１００
データA
184
廃棄

【図１８】


クライアント
(端末A)
18
19
サーバ
(端末B)
10
ルータ
TCPデータセグメント
・シーケンス番号＝１００
データA
191
TCPデータセグメント
・シーケンス番号＝１５０
データB
192
パケットロス
TCPデータセグメント
・シーケンス番号＝２００
データC
193
廃棄
TCPデータセグメント
・シーケンス番号＝２５０
データD
194
廃棄
送達確認セグメント
・確認応答番号＝１５０
195
データA
の
送達確認
TCPデータセグメント
・シーケンス番号＝１６０
データB
196
TCPデータセグメント
・シーケンス番号＝２００
データC
197
TCPデータセグメント
・シーケンス番号＝２５０
データD
198
送達確認セグメント
・確認応答番号＝８００
199
データB～
データD
の
送達確認

【図１９】


送信先IPアドレス
宛先IPアドレス
IDENTフィールド
203
202
201
経路制御
データベース手段
フラグメント
識別用記憶領域
中継判定
処理手段
200
209
局A
ネットワーク
インタフェースA
204
205
ネットワーク
インタフェースB
207
206
220 フラグメントされた
IPパケットの先頭
211
IPルータ
229 フラグメントされた
IPパケットの末尾
208
局B
210